UNIVERSITY OF THE AEGEAN

School of Engineering
Department of Information & Communication Systems Engineering
Karlovassi, Samos
Greece

Doctoral Dissertation

Analysing Information Security Behaviour: Technological-Organisational-Individual Framework and Practical Guidelines to Enhance ISP Compliance

by

Ioanna-Aikaterini Topa

August 2019

Advising Committee

Maria Karyda, Associate Professor, Supervisor
Department of Information & Communication Systems Engineering
University of the Aegean

Lilian Mitrou, Professor, Advisor
Department of Information & Communication Systems Engineering
University of the Aegean

Spyros Kokolakis, Associate Professor, Advisor
Department of Information & Communication Systems Engineering
University of the Aegean

Approved by the Examining Committee

Maria Karyda,
Associate Professor, University of the Aegean

Lilian Mitrou,
Professor, University of the Aegean

Spyros Kokolakis,
Associate Professor, University of the Aegean

Georgios Kambourakis,
Associate Professor, University of the Aegean

Konstantinos Lambrinoudakis,
Professor, University of Piraeus

Stefanos Gritzalis,
Professor, University of Piraeus

Panagiotis Rizomiliotis,
Assistant Professor, Harokopio University

Karlovassi, Samos, Greece
September 2019

Acknowledgements

This PhD research which was sponsored by the “IPATIA” grant provided by the University of the Aegean, Greece, has been completed under the supervision and guidance of Maria Karyda, Associate Professor at the University of the Aegean. I would like to thank my supervisor for her guidance, support, useful insights and knowledge about Scientific research and Information Systems Security Management that she has given me all these years.

I would also like to thank Lilian Mitrou, Professor at the University of the Aegean, for passing me her knowledge on Legal Informatics and Data Protection and for teaching me that I need to be focused on my goals and try for the best.

Furthermore, I would like to thank the Professors Stefanos Gritzalis, Konstantinos Lambrinoudakis, the Assosiate Professors Spyros Kokolakis, Georgios Kambourakis and the Assistant Professor Panagiotis Rizomiliotis for the knowledge that have passed on me during my studies and for providing me with a comprehensive understanding of Information Systems Security, which helped me develop an interest for research in this field.

Finally, I would like to thank my parents, my sister Evangelia, Giorgos, Spyridoula and Lynne, for their love, continuous encouragement, help and support all these years. They facilitated and encouraged me to follow my goals and dreams and complete my PhD.

Contents

Table of Figures

List of Tables

Περίληψη

Η ραγδαία ανάπτυξη της τεχνολογίας οδήγησε σε νέες απειλές και αδυναμίες ασφάλειας καθώς και στην επιβολή του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων σύμφωνα με τον οποίο οι οργανισμοί θα πρέπει να συμμορφώνονται με τις ρυθμιστικές του διατάξεις και να εφαρμόζουν ασφάλεια και ιδιωτικότητα by design (Karyda & Mitrou, 2016; Mitrou, 2017a), συνεπώς η σωστή και αποτελεσματική συμπεριφορά ασφάλειας των υπάλληλων είναι πιο αναγκαία από ποτέ. Παρά το γεγονός ότι οι οργανισμοί επενδύουν σημαντικά χρηματικά ποσά για την εφαρμογή μέτρων ασφάλειας, συγγραφής και υλοποίησης πολιτικών ασφάλειας για την προστασία των πληροφοριακών αγαθών και πόρων ώστε να διασφαλίσουν τον οργανισμό από οικονομική ζημία ή άλλους είδους καταστροφή, εξακολουθούν να πραγματοποιούνται περιστατικά ασφάλειας, ως απόρροια της αποτυχίας των εργαζομένων να συμμορφωθούν με τις πολιτικές ασφάλειας (Bulgurcu et al., 2010).

Επομένως δεν λαμβάνεται υπόψη ο «ανθρώπινος παράγοντας» στον τομέα της ασφάλειας στους οργανισμούς και δεν είναι κατανοητό το πως μπορεί να επιτευχθεί σωστή συμπεριφορά ασφάλειας από την πλευρά των εργαζομένων. Προκειμένου να αντιμετωπιστεί το κενό αυτό, η παρούσα διδακτορική Διατριβή έχει ως στόχο να απαντήσει σε δυο βασικά ερευνητικά ερωτήματα: α) ποιοι παράγοντες επηρεάζουν τη συμπεριφορά ασφάλειας των εργαζομένων και β) πώς μπορεί η γνώση αυτή των παραγόντων να χρησιμοποιηθεί ώστε να βοηθήσει τους security managers (υπεύθυνους διαχείρισης ασφάλειας) να βελτιώσουν τις πρακτικές διαχείρισης ασφάλειας και να ενθαρρύνουν τη συμπεριφορά ασφάλειας εργαζομένων να εναρμονιστεί με τις απαιτήσεις και τους στόχους ασφάλειας του οργανισμού.

Προκειμένου να απαντηθεί το πρώτο ερευνητικό ερώτημα, πραγματοποιήθηκε ανάλυση και κριτική ανασκόπηση της σχετικής βιβλιογραφίας ώστε να εντοπιστούν όλοι οι παράγοντες που επηρεάζουν τη συμμόρφωση με τις πολιτικές ασφάλειας και τη συμπεριφορά ασφάλειας. Μέσα από την ανάλυση της σχετικής βιβλιογραφίας, εντοπίστηκε μια πληθώρα από διαφορετικούς παράγοντες, οι οποίοι όμως δεν είναι κατανοητοί και χρήσιμοι για τους security managers για πολλούς λόγους: συχνά παρουσιάζονται παράγοντες με αντικρουόμενα αποτελέσματα, όπως συμβαίνει για παράδειγμα με τις κυρώσεις, χρησιμοποιούνται διαφορετικοί όροι για να περιγράψουν παρόμοιες έννοιες δημιουργώντας σύγχυση και δυσκολία στην κατανόηση τους, όπως για παράδειγμα στην περίπτωση των όρων αυστηρότητα τιμωρίας (punishment severity) και αυστηρότητα αποτροπής (deterrent severity), επίσης η χρήση εξειδικευμένης ορολογίας δημιουργεί επιπρόσθετη δυσκολία καθώς η ορολογία αυτή χρησιμοποιείται σε θεωρίες με τις οποίες οι security managers δεν είναι εξοικειωμένοι, όπως αυτό-αποτελεσματικότητα (self-efficacy) και συσχέτιση αξίας (value congruence).

Επιπρόσθετα ένα σημαντικό εύρημα της ανάλυσης της βιβλιογραφίας είναι ότι ενώ ο ρόλος της τεχνολογίας και τα χαρακτηριστικά της επηρεάζουν τη συμπεριφορά ασφάλειας, ωστόσο δεν έχουν μελετηθεί επαρκώς στη σχετική βιβλιογραφία. Προκειμένου να μελετηθούν περαιτέρω οι τεχνολογικοί παράγοντες που επηρεάζουν τους χρήστες να χρησιμοποιήσουν εργαλεία ασφάλειας και ιδιωτικότητας, πραγματοποιήθηκε έρευνα ανάμεσα σε 150 φοιτητές των Πληροφοριακών και Επικοινωνιακών συστημάτων ώστε να μελετηθεί η ευχρηστία των εργαλείων ασφάλειας και ιδιωτικότητας. Ένας συνδυασμός από διαφορετικές μεθόδους χρησιμοποιήθηκαν περιλαμβάνοντας σενάρια, ερωτηματολόγια και συνεντεύξεις. Τα ευρήματα δείχνουν ότι οι χρήστες θεωρούν σημαντικά χαρακτηριστικά ευχρηστίας όπως προσβασιμότητα (accessibility), χρήση κατανοητής γλώσσας, intuitiveness, απόδοση, ανατροφοδότηση και λάθη, αποτροπή σφαλμάτων, αναίρεση ενεργειών, διαθεσιμότητα πληροφορίας, design και συνέπεια, χαρακτηριστικά σχετικά με την εγκατάσταση, χαρακτηριστικά σχετικά με την ιδιωτικότητα (έλεγχος προσωπικών δεδομένων και διαφάνεια) και αυτοματοποίηση.

Με βάση τα ευρήματα της ανασκόπησης της βιβλιογραφίας και της έρευνας, δημιουργήθηκε ένα πλαίσιο παραγόντων που επηρεάζουν τη συμπεριφορά ασφάλειας. Το πλαίσιο που αποτελείται από τους παράγοντες της βιβλιογραφίας ταξινομημένους σε τρεις κατηγορίες μαζί με την ανάλυση της σημασίας και της επίδρασης τους, διευκολύνει τους security managers να αντιμετωπίσουν το πολύπλοκο ζήτημα της συμπεριφοράς ασφάλειας. Το πλαίσιο αυτό παρουσιάζει μια συνολική ανάλυση όλων των παραγόντων που επηρεάζουν τη συμπεριφορά ασφαλείας, ταξινομημένους σε τρεις κύριες κατηγορίες που αφορούν ατομικές, οργανωτικές και τεχνολογικές πτυχές. Ο σκοπός αυτού του πλαισίου είναι να λειτουργήσει ως «οδηγός» για τους security managers παρουσιάζοντας τους παράγοντες που πρέπει να λαμβάνουν υπόψη κατά το σχεδιασμό και την υλοποίηση των πολικών και πρακτικών ασφάλειας.

Στη συνέχεια, η πρακτική αξία αυτού του πλαισίου διερευνήθηκε περαιτέρω με την ανάλυση των πρακτικών διαχείρισης ασφάλειας που προβλέπονται στα πρότυπα ISO / IEC 27000, πιο συγκεκριμένα ISO 27001, 27002, 27003 και 27005. Μέσω μιας ανάλυσης εντοπισμού κενών και ελλείψεων, εντοπίστηκαν παράγοντες που επηρεάζουν τη συμπεριφορά ασφαλείας, που όμως δεν περιλαμβάνονται στα πρότυπα ISO, συμπεριλαμβανομένης της συμμετοχής της ανώτατης διοίκησης, της κουλτούρας (culture), του κόστους συμμόρφωσης, των συνηθειών, των ατομικών χαρακτηριστικών και των αξιών. Επιπλέον, παρέχεται πρακτική καθοδήγηση σχετικά με τον τρόπο ενσωμάτωσης της τρέχουσας διαχείρισης της ασφάλειας με πρακτικές που υποστηρίζουν τη συμπεριφορά ασφάλειας.

Για να μελετηθεί και να διαπιστωθεί η δυνατότητα εφαρμογής του πλαισίου, πραγματοποιήθηκε μια μελέτη περίπτωσης σε έναν μεγάλο οργανισμό. Η μελέτη περίπτωσης είχε ως στόχο την ανάλυση των τρεχουσών πρακτικών διαχείρισης της ασφάλειας του οργανισμού και τον προσδιορισμό των πτυχών του πλαισίου που εφαρμόζονται στην πράξη. Μέσω αυτής της μελέτης περίπτωσης ήταν δυνατό να προσδιοριστούν οι πρακτικές διαχείρισης της ασφάλειας που εφαρμόζονται και να αποκτηθούν γνώσεις σχετικά με τις πρακτικές που ακολουθούνται από τον οργανισμό. Ένα σημαντικό συμπέρασμα είναι ότι αυτός ο οργανισμός υποστηρίζει την τηλεργασία και έχει αναγνωρίσει τη σημασία της ενημέρωσης των χρηστών σχετικά με τις απειλές και τους κινδύνους που μπορεί να προκύψουν κατά την τηλεργασία, σχεδιάζοντας για το σκοπό αυτό νέες πολιτικές ασφάλειας. Αυτό υπογραμμίζει την ανάγκη που υπάρχει ώστε οι οργανισμοί να είναι ενήμεροι για τη συνεχή εξέλιξη της τεχνολογίας, τον αντίκτυπό της στον εργασιακό χώρο και την επακόλουθη ανάγκη ανανέωσης των πρακτικών ασφάλειας τους. Επιπλέον, η μελέτη περίπτωσης προσφέρει στοιχεία για το πώς ένας οργανισμός μπορεί να παρακινήσει τους εργαζομένους να υιοθετήσουν την κατάλληλη συμπεριφορά ασφαλείας: πρώτον, με τη χρήση πρακτικών μεθόδων όπως κάρτες ή αφίσες. Δεύτερον, προωθώντας μια οργανωτική κουλτούρα ασφάλειας η οποία βασίζεται στην επικοινωνία, στις κοινές αξίες και στην αλληλοβοήθεια. Τέλος, η μελέτη περίπτωσης αποκαλύπτει πως η στάση του συγκεκριμένου οργανισμού σχετικά με τις κυρώσεις (δεν εφαρμόζονται κυρώσεις για τη μη συμμόρφωση των πολιτικών ασφάλειας παρά τις συστάσεις του ISO) μπορεί να είναι η καταλληλότερη πολιτική για τον οργανισμό αυτό. Εκτός από την παροχή προτάσεων για περαιτέρω βελτίωση των πρακτικών διαχείρισης της ασφάλειας, η μελέτη περίπτωσης καταλήγει επίσης στο συμπέρασμα ότι, υπάρχει ανάγκη για εφαρμογή πρακτικών διαχείρισης της ασφάλειας που να είναι προσαρμοσμένες και να ταιριάζουν στις ανάγκες και τις απαιτήσεις της ασφάλειας των πληροφοριών των οργανισμών, λαμβάνοντας υπόψη και εκμεταλλευόμενες τα βασικά δυνατά σημεία τους.

Τέλος, με βάση τα ερευνητικά ευρήματα, τη μελέτη για την ευχρηστία, την ανάλυση για τον εντοπισμό κενών των προτύπων ISO και την μελέτη περίπτωσης, η παρούσα διατριβή πληροί τον δεύτερο ερευνητικό στόχο παρέχοντας πρακτικές οδηγίες, ώστε οι security managers να κατανοήσουν καλύτερα τη συμπεριφορά ασφαλείας και να ενισχύσουν τις τρέχουσες πρακτικές διαχείρισης της ασφάλειας. Αυτό το σύνολο των πρακτικών οδηγιών επικεντρώνεται κυρίως στο πως μπορούν οι security managers να υιοθετήσουν στην πράξη τους παράγοντες που επηρεάζουν τη συμπεριφορά ασφάλειας των εργαζομένων και έχουν εντοπιστεί στη βιβλιογραφία όπως επίσης και παράγοντες που δεν αντιμετωπίζονται επαρκώς ούτε στην τρέχουσα βιβλιογραφία ούτε/ και στα ευρέως υιοθετημένα πρότυπα ISO.

Η μελέτη αυτή συμβάλλει στον τομέα της συμπεριφοράς ασφάλειας και συμμόρφωσης με τις πολιτικές ασφάλειας μέσω:

α) του καθορισμού και της ανάλυσης των αντικρουόμενων αποτελεσμάτων και της σύγχυσης της ορολογίας στη σχετική βιβλιογραφία,

β) της αιτιολόγησης του ρόλου της τεχνολογίας για τη διαμόρφωση της συμπεριφοράς ασφαλείας και την ανάλυση σχετικών παραγόντων που επηρεάζουν τη χρήση των εργαλείων ασφάλειας και ιδιωτικότητας. Επίσης τεκμηριώνεται η ανάγκη για τους προγραμματιστές να εξετάσουν τα χαρακτηριστικά χρηστικότητας που εντοπίστηκαν προκειμένου να σχεδιάσουν εργαλεία ασφάλειας που μπορούν να είναι εύχρηστα.

γ) της παροχής οδηγιών για την ενίσχυση της διαχείρισης της ασφάλειας, με στόχο την αντιμετώπιση των κενών στις τρέχουσες προσεγγίσεις διαχείρισης της ασφάλειας σύμφωνα με τα πρότυπα ISO 27001, 27002, 27003 και 27005. Οι παράγοντες που δεν καλύπτονται από τα παραπάνω πρότυπα ασφάλειας σχετίζονται με τη συμμετοχή της ανώτατης διαχείρισης, την κουλτούρα, το κόστος συμμόρφωσης, τις συνήθειες, τα ατομικά χαρακτηριστικά, τις ικανότητες, τις αξίες, τα διάφορα είδη συνειδητοποίησης της ασφάλειας και την κοινωνική επιρροή.

Συνολικά, αυτή η διδακτορική διατριβή γεφυρώνει το χάσμα ανάμεσα στη θεωρία και την πράξη, παρέχοντας στους security managers έναν «οδηγό», με τη μορφή πλαισίου τριών κατηγοριών και ενός συνόλου οδηγιών για τη βελτίωση της συμπεριφοράς ασφαλείας και της συμμόρφωσης των εργαζομένων με τις πολιτικές ασφάλειας. Συνολικά, η παρούσα μελέτη αποτελεί έναν «οδηγό» για το πως μπορούν οι security managers να λάβουν υπόψη τις ατομικές, οργανωτικές και τεχνολογικές πτυχές της συμπεριφοράς ασφάλειας κατά την υλοποίηση των πρακτικών διαχείρισης ασφάλειας και να βελτιώσουν τη συμμόρφωση των εργαζομένων με τις πολιτικές ασφάλειας.

Τέλος, καθώς ο τομέας της ασφάλειας πληροφορικής είναι σύνθετος και εξελίσσεται ταχύτατα εξαιτίας της ανάπτυξης νέων τεχνολογιών και της αλλαγής του τρόπου εργασίας, είναι επιτακτική η ανάγκη να ερευνηθεί περαιτέρω ο ανθρώπινος παράγοντας όπως επίσης και ο ρόλος της τεχνολογίας για τη διαμόρφωση της συμπεριφοράς ασφαλείας.

Executive Summary

With the advancement of technology leading to new security threats and vulnerabilities and the enforcement of the General Protection Regulation (GDPR) according to which organisations must be compliant with its regulatory requirements and implement security and privacy by design (Karyda & Mitrou, 2016; Mitrou, 2017a), effective employee security behaviour is needed more than ever. Moreover, organisations invest heavily in security countermeasures, designing information security policies (ISPs) to protect their information assets and to safeguard against financial loss or other damage to their organisation, and yet security incidents continue to occur, often as a result of employees' failure to comply with information security policies (Bulgurcu et al., 2010). In short, there is a clear gap in organisations addressing the "human aspect" of security and understanding of how to achieve the appropriate security behaviour from their employees. In order to address this gap, this Thesis aims to answer two main research questions: a) which factors influence employee security behaviour; and b) how knowledge of these factors can be exploited to help security managers enhance security management practices and thus encourage employee security behaviour to be in line with the organisation's security objectives.

With the first research objective in mind, a critical analysis and review of relevant literature was carried out to identify all factors influencing ISP compliance and security behaviour. After analysing relevant literature, it was identified that there is a plethora of different factors, which, while useful, are not comprehensible or useful to security managers for a variety of reasons: they often present unclear or conflicting results, such as the effect of sanctions ; different terms are used to describe similar concepts adding confusion to the field, as in the case of punishment severity (or deterrent severity) and in the case of resource availability and facilitating conditions; also, specialised terminology used is often confusing as it is drawn from theories that security managers are unlikely to be familiar with, such as self-efficacy, perceived value congruence etc.

Furthermore, an important finding of the analysis of related literature was that the role of technology and its characteristics affect security behavior however their role is not adequately studied and addressed in relevant literature. To further explore the technological factors that influence users to use security and privacy tools a survey was conducted among 150 ICT Students to investigate the usability of security and privacy tools. A combination of different research instruments was employed in this survey including scenarios, questionnaires and interviews. Findings show that users value usability security characteristics such as

accessibility, language, intuitiveness, efficiency, feedback and errors, error prevention, undo actions, availability of information, design and consistency, characteristics relevant to installation, privacy characteristics and automation.

Based on the findings from the literature review and the survey, a framework of factors influencing security behaviour was created. The framework which consists of these factors grouped into three categories along with the analysis of their implications facilitate security management address the multi-faceted issue of security behaviour. This framework presents a comprehensive analysis of all factors that influence security behaviour, classified under three main categories addressing individual, organisational and technological aspects. The aim of this framework is to act as a roadmap of the different factors that security managers need to consider when designing and implementing ISPs.

Subsequently, the practical value of this framework was further investigated by analysing current security management practices provisioned in the ISO/IEC 27000 series, namely ISO 27001, 27002, 27003 and 27005. Through a gap analysis several factors influencing security behaviour were identified, which are not addressed in the ISO Standards, including top management participation, cultural context, cost of compliance, habits, individual characteristics and values. Furthermore, practical guidance is provided on how to integrate current security management with practices that support security behavior.

To validate the applicability of the framework a case study was performed in a large organisation. The case study aimed to analyse the current security management practices of the organisation and to identify aspects of the framework that were implemented. Through this case study it was possible to identify the security management practices that are currently applied and gain insights into the practices followed in the day-to-day running of the organisation. An important finding is that this organisation supports teleworking and has recognised the importance of informing users about the threats and risks that might take place during teleworking by designing new ISPs for this purpose. This highlights the need for organisations to be aware of the constant evolution of technology, its impact on the workplace and the resulting need to update their practices accordingly. Furthermore, the case study offers additional insights into how an organisation may motivate employees to adopt the appropriate security behaviour: firstly, through the use of practical methods such as cards or posters; secondly by promoting an organisational information security culture of communication, common values and openness. Finally, the case study reveals how this organisation's individual stance on sanctions (no sanctions are applied for ISP non-compliance despite ISO recommendations) may be the most appropriate policy for this organisation. Besides providing suggestions for further enhancement of security management practices, the case study also

concludes that in terms of employee security behaviour there is a need for more customised security management practices to suit the information security needs of particular organisations rather than a one-size-fits-all approach.

Finally, drawing from research findings, the usability study, the ISO Standards gap analysis and the case study, this Thesis meets the second research objective by providing practical guidelines, to enable security managers to better understand security behaviour and enhance their current security management practices. This set of guidelines focuses principally on those areas which findings from the present study have identified as both significant factors influencing employee security behaviour and factors which are insufficiently addressed either in current literature and/or the widely adopted ISO standards.

This Thesis contributes to the field of security behaviour and ISP compliance by:

a) identifying and analysing conflicting results and confusing terminology in related literature,
b) justifying the role of technology for shaping security behaviour and analysing relevant factors that influence the use of security and privacy controls. It also identifies the need for developers to consider the usability characteristics identified in order to design usable security tools.
c) providing guidelines to enhance security management and addressing the gaps in current security management approaches following ISO 27001, 27002, 27003 and 27005 Standards with regard to top management participation, the cultural context, cost of compliance, habits, individual characteristics, perceptions about threats and capabilities, values, different types of security awareness and social influence.

Overall, this Thesis bridges the gap between theory and practice by providing security management a roadmap, in the form of a three categories framework and a set of applicable, as shown through the case study, guidelines to enhance security behaviour and ISP compliance. Overall, this Thesis provides a roadmap to address the individual, organisational and technological aspects of security behaviour that can lead to improved ISP compliance.

Finally, as the field of information security is highly complex and undergoing rapid changes as a result of new technologies and changing work styles, we conclude that there is a standing need for further research into the role of the human aspects of information security and the role of technology for shaping security behaviour.

Chapter 1: Introduction to Information Security Behaviour

1.1 Information Security Policy Compliance and Security Behaviour: Background

Organisations implement security countermeasures to preserve confidentiality, integrity and availability of their data and systems. They also have Information Security Policies (ISPs) in place, which are defined as "the statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" (Bulgurcu et al., 2010). Security policies refer to a variety of different security related aspects, e.g. password requirements, cryptography controls, monitoring mechanisms, security training and awareness, roles and responsibilities of the employees, security controls, access management, privileged access management, etc. ISP compliance is described as the action of employees following their organisation's ISPs to achieve optimum information security and safeguard organisational assets and data. When an individual is aware of security threats and vulnerabilities, follows security practices, processes and rules, and uses security tools, then he/she forms a security behaviour.

Due to the advancement and complexity of new technologies which have resulted in an increase in the number and severity of security threats, following the appropriate security behaviour is challenging and although organisations invest in implementing ISPs and security tools, there are numerous cases cited where employees have caused security breaches (Redteam, 2018). Among the organisations that faced cybersecurity incidents in 2017, one-in-ten (11%) the most serious types of incidents involved careless employees (Kaspersky report, 2017). Furthermore, careless and unaware employees were identified as the biggest security vulnerability with the most increased risk exposure during the year 2018-2019 (EY Global Information Security Survey, 2019). For this reason, employees are often regarded as the weakest link in organisations' information security. Security breaches attributed to "human error" (Ponemon Institute, 2012, p.7) are caused because individuals do not use security tools or circumvent them and fail to comply with ISPs, putting their organisation at risk. Research suggests that employees fail to use security tools effectively and do not follow ISPs (Safa et al., 2016) for a variety of reasons, e.g. due to the difficulty of dealing with the complex requirements of information security (Cranor & Buchler, 2014), the inconvenience of spending time following security practices (Vance et al., 2012), etc.

ISP non-compliance on the part of employees can result in significant problems for an organisation, including financial losses and damage to the organisation's reputation. To prevent

such problems arising, organisations must therefore find ways to motivate their employees to comply with those ISPs and to apply the use of more effective security tools in order to avoid security incidents. However, while there is focus in literature and the ISO Standards followed by many organisations on the security countermeasures which organisations may implement to secure their information assets, the "human aspect" is overlooked (Crossler et al., 2013, Dhillon & Torkzadeh, 2006, Bulgurcu et al., 2010). Thus, the heart of the problem is the lack of understanding on the part of security managers regarding what motivates employees to form a security behaviour. Literature provides a wealth of useful insights on the factors that motivate users to comply with ISPs (Pahnila et al., 2007; Siponen et al., 2006; Siponen et al., 2014; Ifinedo, 2012; Vance et al., 2012; Pahnila et al., 2013; D'Arcy et al., 2009; Bulgurcu et al., 2010; Myyry et al., 2009; Herath & Rao, 2009a; Herath & Rao, 2009b; Ifinedo, 2014; Safa et al., 2016; Son, 2011; Hu et al., 2012; D'Arcy & Greene, 2014; Moody et al., 2018). These factors derive from various theories of psychology, sociology, criminology and aim to inform security managers about the effect of these factors on security behaviour and ISP compliance in order to design their security management practices appropriately.

Security management practices are based on widely accepted international standards for security such as the ISO 27000 family of standards including ISO 27001, 27002, 27003 and 27005. However, these standards are generic in nature, giving rise to possible lack of understanding or applicability. While there is a number of research papers on these standards that aim to inform security managers and explain ISO standards, their aims and practices more thoroughly to security managers (Tsohou et al., 2009; Tsohou et al, 2010) they do not draw on the findings of the different theories, or focus mainly on applying the principles of deterrence theories such as General Deterrence Theory and other crime theories on ISO Standards (Coles-Kemp & Theoharidou, 2010).

According to Spyridopoulos et al. (2014), when principles from the Viable System Model, which is grounded in Systems Theory are combined with an IT Risk Analysis, more security threats and vulnerabilities can be identified. Furthermore, this shows that theoretical research findings can provide security managers with insights which they might otherwise not consider. Furthermore, However, due to limited time, resources and understanding of the relevant theories, security managers are unlikely to benefit from these insights without the appropriate guidance. For this reason, this PhD Thesis aims to provide an overview of the multitude of factors that influence employees' security behaviour, create a framework based on these factors and then suggest how current Information Security Management Practices based on ISO/IEC Standards can be improved when these factors are considered. Without the relevant information and a clearer understanding of this complex field, security managers

cannot design and implement user-friendly security management practices that will lead to improved ISP compliance and employees adopting a security behaviour that is aligned with their organisation's security objectives. This Thesis aims to address this gap, providing security managers with a roadmap and handbook for practical guidance.

To address this issue, the present Thesis aims to answer the following research questions:

- Which factors influence the security behaviour of employees?
- How can the knowledge about these factors be exploited so as to enhance security management practices?

To address the first research question a thorough review and analysis of related literature in the field of information security behavior was conducted, in order to establish a comprehensive picture of all the documented factors related to security behavior (Topa & Karyda, 2015; Topa & Karyda, 2016); through this analysis areas were identified that are not sufficiently explored, such as the role of usability of security technology. This aspect was further explored through a usability survey (Topa & Karyda, 2018). By combining the findings from both the literature review and the survey a Technological-Organisational-Individual framework is developed.

To address the second research question, a clear picture of the security management practices that are currently implemented in organisations was needed. As most organisations adhere to the widely accepted international standards, including the ISO family of standards- particularly ISO 27001, 27002, 27003 and 27005- this Thesis conducts a gap analysis of these standards to enable a comparison between literature findings and current practices, and provide directions and guidelines to address the identified gaps (Topa & Karyda, 2019). Moreover, a case study was conducted to investigate the security management practices followed in a large organization and show how the knowledge on factors influencing security behavior can be incorporated into security management practices to improve ISP compliance and the overall security posture of organisations.

1.2 General Conclusions

The main conclusion of this Thesis is that when dealing with issues of security behaviour and ISP compliance, organisations need to adopt a comprehensive perspective addressing all three categories of security behaviour factors, namely individual, organisational

and technological. These three categories are interdependent and interconnected. Therefore, to facilitate ISP compliance security managers should limit their focus on considering only some of these factors, but they need to consider the whole spectrum of the identified factors. They should also identify the key strengths of their organisations and design their security management practices in such a way that they can benefit from these key strengths to promote ISP compliance.

While the field of information security is well-documented and researched and there is a significant body of literature available, this Thesis reveals the challenging task for most security managers of navigating within the often bewildering array of terms and theories and contrasting findings. At the same time, overly generic guidelines as laid down in ISO standards may also present security managers with difficulties as this Thesis concludes that information security needs to be tailored to meet the specific security objectives of a particular organisation and be aligned with its organisational culture and values.

1.3 Contribution of the Thesis

Based on a thorough review of literature in the field of information security, this Thesis compiles a comprehensive list of factors which influence users' security behaviour. Particular problem areas are identified, highlighting the need for clarification and further study. These include overlapping concepts, confusing terminology and conflicting results.

In addition, drawing on the widely held view that the human aspect of information security is not adequately addressed (Bulgurcu et al., 2010) this Thesis offers useful insights into users' perceptions through a usability survey of security tools.

As one of the main objectives of the present Thesis is to facilitate security management practices, this Thesis presents a clear, accessible three-category framework of factors to serve as a roadmap for security managers, enabling them to better navigate within highly complex field of security behaviour and enhance their practices.

Mapping the relevant ISO Standards concerning security behaviour against this Technological-Organisational-Individual framework assists in identifying limitations of security management practices and gaps between recommended practices and current literature. Moreover, applying the framework in a case study confirms its applicability. This framework can be used as a roadmap by security managers and reveals further insights into how security management is carried out in practice.

Building on the findings from literature as well as the insights gained from the usability survey, the gap analysis of ISO standards and the case study, this research develops a handbook

or set of guidelines for security managers to follow that will both improve their awareness and understanding of security behaviour and offer practical ways to enhance their security management practices and in turn ISP compliance.

	Contribution	Publications	Reference
1	Application of the Technological-Organisational-Individual framework of security behaviour factors in a large organisation, analysis of current practices and recommendations	I. Topa, M. Karyda. A Case Study: Addressing Organisational, Individual and Technological aspects in information security management	(to be submitted)
2	Analysis of current security management practices based on literature findings and development of a set of practical guidelines	I. Topa, M. Karyda, From Theory to Practice: Guidelines for Enhancing Information Security Management, Emerald Publishing, Journal of Information and Computer Security	(Topa & Karyda, 2019)
3	Exploration and analysis of usability characteristics from the user's perspective through HCI literature review and survey	I. Topa, M. Karyda, Usability Characteristics of Security and Privacy Tools: The User's Perspective, 33rd IFIP TC 11 International Conference, SEC 2018 Held at the 24th IFIP World Computer Congress, WCC 2018, September 2018, Poznan, Poland	(Topa & Karyda, 2018)
4	Analysis of security behaviour determinants and creation of the Technological-Organisational-Individual framework	I. Topa, M. Karyda, Analyzing Security Behaviour Determinants for enhancing ISP Compliance and Security Management, 13th European,	(Topa & Karyda, 2016)

		Mediterranean and Middle Eastern Conference on Information Systems (EMCIS), 2016, Krakow, Poland	
5	Analysis of current literature and identification of factors influencing employee security behaviour and ISP compliance	Topa, I., & Karyda, M. (2015) Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. Trust, Privacy and Security in Digital Business. Springer International Publishing.	(Topa & Karyda, 2015)
6	Application of Viable System Model Theory to an organisation in conjunction with IT Risk Analysis to enhance security protection	Spyridopoulos, T., Topa, I., Tryfonas, T. & Karyda, M. (2014) A Holistic Approach for Cyber Assurance of Critical Infrastructure through Viable System Modelling. IFIP SEC 2014, Springer Berlin Heidelberg	(Spyridopoulos, Topa, Tryfonas & Karyda, 2014)

Table 1: List of publications and Thesis contribution

1.4 Structure of the Thesis

Chapter 1 introduces the purpose of this Thesis, giving background information and providing definitions of relevant concepts, as well as outlining the need for research and the main research aims of the Thesis.

Chapter 2 presents the literature review of security behaviour determinants. In order to answer the initial research question of this Thesis-namely, which factors influence security behaviour-the starting point for the research was a comprehensive and analytical review of current literature in the field of security behaviour and ISP compliance. This extensive review finds that security behaviour constitutes a highly complex field of study and hence there is a need to classify and clarify the factors involved. It also identifies a lack of information concerning the role of technology and its influence on security behaviour, which prompted a

further, more in-depth review of usability factors. Thus, Section 2 begins with the general literature review, followed by the usability review with its special focus on technological aspects. It then concludes with a summary of the main findings and a table containing all the factors identified from literature.

In Chapter 3 the research design is described showing all the different phases of the research and the research methodology employed in each stage. The phases include the literature review, a usability survey with questionnaires and interviews, the development of a framework of factors, an analysis of ISO Standards (ISO 270001, 27002, 27003 and 27005), a case study to test the applicability of the framework and gain insights into security management in practice and a set of practical guidelines for security managers on how to design their security management practices.

Chapter 4 presents the usability survey, the next stage in researching the role of technological factors. This section begins with an introduction which outlines the rationale behind this survey as well as justification for some of the methods used. This is followed by a description of the method of collecting data and a description of the scenarios used in the survey. The different factors that were identified in the literature and derive mainly from the usability heuristics of Nielsen and studies in Human Computer Interaction Security (HCI-SEC) were assessed by users in terms of their importance to them. Users were asked to install a security or a privacy tool on their computers and follow a scenario, then complete a questionnaire and participate in interviews to give their views and perceptions about the usability of the security and privacy tools they used. Findings are then reported according to the usability characteristic they refer to, presented in a table and finally analysed in detail in the conclusions. By conducting the survey in this way it was possible to obtain a clear picture of the user's perspective on technological aspects to add to the findings of previous research.

Chapter 5 presents the Technological-Organisational-Individual framework. Findings from the initial literature review revealed the complexity of security behaviour as a field of study. In order to address the second major research question of this Thesis-i.e. how to exploit the factors involved in security behaviour to enhance security management practices-a more concise and more easily accessible overview of security behaviour factors was created in the form of a comprehensive framework of individual, organisational and technological factors that influence individuals to form a security behaviour. This Technological-Organisational-Individual framework shows the different factors presented in a user-friendly way which is easy for security managers to comprehend and to be able to make use of when designing their security management practices. To further support understanding of the framework, a brief description follows explaining the role of the relevant factors in each category.

Chapter 6 includes a description and analysis of current guidelines/recommendations for security management as laid down by the ISO/IEC Standards, 27001 27002, 27003 and 27005. This section continues by mapping the proposed framework against these ISO/IEC Standards to identify which factors are not adequately incorporated in current security management guidelines. A clearer understanding of the shortcomings of current practices would help answer the second research question of this Thesis and provide the foundation for the development of a new set of improved guidelines. The section concludes by summarising the main limitations of the ISO Standards for security management practices.

Chapter 7 presents the case study conducted in a large organisation to determine the security management practices of a real organisation, applying the framework to identify any shortcomings and make any recommendations for improvement. Firstly, there is an introduction with relevant details concerning the organisation followed by a description of the research methods used. The section continues with an analysis of the security management practices that are currently implemented in the organisation. Finally, a set of recommendations for additional or improved practices is described and also presented in a table, together with new insights gained from the case study, which prove useful in supplementing the next stage of this Thesis.

Chapter 8 presents a set of practical guidelines for security managers to take into account in order to enhance their security management practices. These guidelines are the culmination of all the findings in this research and based on the factors that are included in the framework, with the aim of giving security managers a better understanding of how to design and implement security management practices to achieve ISP compliance. A short conclusion ends the section.

Chapter 9 discusses challenges for security management. Security managers are facing many challenges since they need to consider all the different factors of security behaviour, namely organizational, individual and technological. The main challenges are analysed, especially the discrepancies of what the literature and ISO Standards suggest and what happens in practice. This chapter concludes with the limitations of literature findings, the usability survey and the case study.

Finally, Chapter 10 presents the major findings and conclusions as well as recommendations for future work. The main conclusion of this Thesis is that security managers should adopt a comprehensive perspective by addressing all three categories of factors (organizational, individual and technological) when designing their security management practices in order to achieve ISP compliance.

Chapter 2: Information Security Behaviour Determinants: The Current Landscape

2.1 Introduction

Given that many security breaches are attributed to human error, there is a need to investigate all the factors that influence employees' security behaviour. The primary aim of the literature review in this Thesis was to thoroughly examine current research in order to identify all the factors involved in influencing security behaviour. This analysis was conducted at a wide range of different studies from fields as diverse as psychology, sociology and criminology and comparing the findings. The different studies were based on a multitude of different theories such as the Protection Motivation Theory (Siponen et al., 2006; Pahnilla et al, 2007; Herath & Rao, 2009a; Vance et al., 2012; Siponen et al., 2014; Pahnilla et al., 2013), the Technology Acceptance Model (Dinev & Hu, 2007), the General Deterrence Theory (D'Arcy et al., 2009; Herath & Rao, 2009a; Herath & Rao, 2009b; Son, 2011), the Rational Choice Theory (Bulgurcu et al., 2010), the Social Bond Theory (Safa et al., 2014) etc.

Analysis of related literature also identified areas where there was a lack of clarity or insufficient research to date and thus a need for further detailed study. More specifically, the literature review revealed several overlapping factors and instances of concept confusion or confusing terminology, as well as insufficient research on the role of technology in influencing security behaviour.

While a plethora of organisational and individual factors relevant to security behaviour were identified through the analysis of the literature on ISP compliance and security behaviour, technological factors are only scarcely addressed. More specifically, there were only a few factors which addressed users' perceptions about technology, including perceived ease of use, perceived usefulness and perceived responsiveness. There is a need to extend the search in technology to more specialised areas of research covering Human Computer Interaction and information security. Given the clear connection between the user and the tool-namely, that a security tool can only be effective if used appropriately which is further supported by Johnston et al. (2003) who stated that "the easier a system is to use, the less likely the user will be to make a mistake or to try to bypass the security feature"- it seems essential to investigate users' perceptions regarding the myriad aspects of security tool usability. There is a need to explore the users' perspective, identify their needs and expectations as to which usability factors they consider important and why.

Thus, the next step in the exploration of security behaviour factors was to analyse the more specific body of literature on the usability of security technology to identify and explore the multiple factors involved in motivating individuals to use, or equally deterring them from using, security tools.

2.2 Method of literature review

28 studies on factors influencing security behaviour were identified, through search engines such as Google Scholar and Scopus, using the following keywords: "ISP compliance", "employees' compliance with security policies", "security behavio(u)r", "factors influencing ISP compliance" and "factors influencing security behavio(u)r". Furthermore, the references list of the manually identified papers were examined from which relevant studies were selected.

2.2.1 Factors influencing security behaviour

A plethora of security behaviour determinants were identified from studies focusing mainly on ISP compliance of employees. Many of these factors refer to individuals' perceptions, values and characteristics. Other factors are related to the security management practices of the organisation, e.g. sanctions and rewards, SETA programs, etc. Finally, there are studies focusing on the technological aspects and what factors influence users to use security tools.

Threat appraisal is a factor influencing employees' intention to comply with ISPs according to (Siponen et al., 2014; Lebek et al., 2014). Threat appraisal consists of *perceived vulnerability* (individuals' perceptions of vulnerabilities and threats) and *perceived severity* (individuals' perceptions about the severity of security threats) (Siponen et al., 2014). Based on this, Pahnila et al. (2007), advocate that employees should be informed about the threats against the organisation and their severity through different means e.g. via seminars, newsletters and posters.

Coping appraisal (individuals' perceptions concerning their competence in complying with ISPs and the effectiveness of ISPs) was studied by Siponen et al. (2014), in terms of *self-efficacy* and *response efficacy*. Employees' *self-efficacy* (defined as individuals' perceptions of how capable they are of following ISPs) was identified as a security behaviour determinant, leading to the suggestion that security managers should provide employees with security education, awareness and training (SETA) programs. *Response efficacy* (defined as individuals' perceptions of whether ISPs are effective in preventing security threats), was

found not to influence security behaviour significantly. However, in other studies (Ifinedo, 2012; Herath & Rao, 2009a) *response efficacy* was identified as a determinant of ISP compliance, suggesting that security managers should expose employees to security technologies and encourage them towards developing the appropriate skills and knowledge. In Herath & Rao (2009a) *response efficacy* has a slightly different meaning and it was defined as perceived effectiveness of ones' actions, showing individuals' perceptions of how they can individually contribute to the organisation if they comply with ISPs.

In another study by Zhang et al. (2009), response efficacy defined as individuals' perceptions on the existence and *effectiveness of security tools* impacts their intention to comply with ISPs negatively, as they believe that when there are effective security mechanisms in place, their security behaviour is less important.

Pahnila et al. (2013) also studied the role of threat and coping appraisal, in conjunction with the degree of employees' *awareness of ISPs*. They found that high-knowledge employees are more likely to adhere to ISPs, as they believe that threats are plausible and real and that non-compliance could lead to severe consequences. Contrary to other studies, in this study self-efficacy has no impact on ISP compliance, suggesting that employees largely rely on security employees' actions to protect organisational assets. Pahnila et al. (2013) show that employee *age* is a security behaviour determinant for employees with high ISP knowledge. Furthermore, (Herath & Rao, 2009b), argue that *gender* is a factor that influences ISP compliance intention, suggesting that females have higher compliance intentions than males.

Vance et al. (2012) consider *benefits to the individual by non-compliance with ISPs* (e.g. time-saving) and *response cost* (e.g. additional effort and time) as factors influencing ISP compliance intention negatively. They argue that security managers need to ensure ISPs and procedures are easy to follow and, more importantly, that they are perceived as easy by employees. Similar to *response cost*, work impediment studied by Bulgurcu et al. (2010) influences *cost of compliance*, which in turn impacts attitude towards ISP compliance negatively. Vance et al. (2012) show that individual *habits* influence security behaviour indirectly, suggesting that security managers need to shape the organisational culture so that employees regard ISP compliance as a necessity and not as an impediment. However, it is not further explained how such perceptions can be instilled.

Another stream of research explores how organisational conditions affect employees' security behaviour and ISP compliance. Pahnila et al. (2007) report that *facilitating conditions* (or *resource availability* as stated in (Herath & Rao, 2009a)), including the availability of resources such as time to become familiar with the ISPs, help from experts and easy access to the ISPs, determine employees' attitude towards ISP compliance (Pahnila et al., 2007). Siponen

et al. (2006) suggest that the *visibility* of information relevant to IS security, through inside and outside resources, affects the security behaviour of employees. Pahnila et al. (2007) identify *information quality* of ISPs as a determinant of employee security compliance.

Employees' awareness of ISPs and of *information security in general* is identified as a determinant of ISP compliance by Bulgurcu et al. (2010). Furthermore, D'Arcy et al. (2009) posit that users' *awareness of security countermeasures*, such as ISPs, SETA programs and monitoring controls, can deter IS misuse. Their study suggests that *perceived severity of sanctions* (individuals' perceptions of the severity of punishment for violating ISPs) is more effective in deterring IS misuse than *perceived certainty of sanctions* (individuals' perceptions on the certainty of being caught for violating ISPs). Contradictory findings for the severity of sanctions are presented by Herath & Rao (2009a), showing that *detection certainty*, namely the visibility and existence of detection mechanisms is more effective than *punishment severity*. They further identify *commitment* to organisational goals as an influential factor of ISP compliance.

Interestingly, according to Son (2011) sanctions do not influence ISP compliance. *Deterrent certainty* (individuals' perceptions about the possibility of getting punished for violating ISPs) and *deterrent severity* (individuals' perceptions about the severe punishment they will receive for violating ISPs) have no impact on security compliance. However, *perceived legitimacy* (individuals' perceptions concerning how fair or just ISPs are), and *value congruence* (the degree to which employees' own values match those of their superiors) are security behaviour determinants. This paper posits that practices that promote intrinsic motivation of employees are more effective than sanctions and underlines the need to connect the objectives of ISPs with employees' values, without however providing any practical guidance. In a similar vein, Hu et al. (2012) advocate that certain managerial approaches, such as *top management participation* (e.g. by contributing to security goals), can shape an organisational security culture and are more effective than deterrence.

On the other hand, Myyry et al. (2009) show that employees comply with ISPs out of *fear of punishment* (a factor which is defined as *preconventional moral reasoning*). They report that employees who are *open to change* (identified as those who follow their own interests and goals) frequently fail to adhere to ISPs. The authors suggest that, while monitoring can be an effective mechanism to ensure ISP compliance, it can be costly, and thus recommend that employees should be encouraged to comply with ISPs out of moral duty. Lowry and Moody (2014) further find that employees who believe that their *freedom is threatened* by ISPs (*threat to freedom*), or those who tend to *react when their freedom is restricted* (*reactance proneness*) will not adhere to a new ISP. *Privacy concerns* seem to have a negative impact on using

security tools (Herath et al., 2014). When users believe that their privacy may be violated, they are likely not to use security mechanisms.

Bulgurcu et al. (2010) identify that *costs* of compliance (including *intrinsic cost* (negative feelings such as shame), *sanctions* and *vulnerability of resources*) impact compliance attitudes and intentions. Additionally, they report that *benefits of compliance (including intrinsic benefit* (positive feelings such as contentment), *rewards* and *safety of resources)* influence employees' attitude and intention towards ISP compliance. However the role of *rewards* as a security behaviour determinant has not been confirmed by similar studies (Siponen et al., 2014; Pahnila et al., 2007). However, the authors assert the view that apart from rewards and sanctions, IS awareness programs should be designed to reinforce employees' beliefs concerning *vulnerability and safety of resources* as well as intrinsic cost and benefit.

Herath & Rao (2009a) report that social influence consisting of *subjective norms* (individuals' perceptions of significant others' expectations e.g. colleagues, superiors, etc.) and *descriptive norms* (individuals' perceptions of significant others' behaviour), are determinants of employees' intentions to comply with ISPs. Ifinedo (2012) suggests that security managers should designate influential people within the organisation to communicate the necessity of ISP compliance. Ifinedo (2014) indicate that social bonds including *involvement* (meaning individuals' participation in meetings and relationships with colleagues who share the same security views), and *commitment*, influence indirectly employees' intention to comply with ISPs. Safa et al. (2016) also find that *commitment* and *involvement*, referring to *knowledge sharing*, *collaboration*, *participation in training programs* (defined as *intervention*) etc. and *experience*, influence ISP compliance. The authors identify impediments in knowledge sharing, as employees are often not willing to share their knowledge.

D'Arcy and Greene (2014) argue that security culture combined with *job satisfaction* can significantly improve ISP compliance. Interestingly, in this study, *perceived organisational support* (individuals' perceptions that the organisation values their contribution and is concerned about their well-being) was negatively related to ISP compliance intention. This can be attributed to employees placing too much faith in the organisation's ability to deal with IS threats even if they themselves fail to do so. Shropshire et al. (2015), on the other hand, report that organisational support is an influential factor for security compliance.

Connolly et al. (2015) found that *organizational culture* influences employees' ISP compliance. Flat management encourages employees to give their feedback about security issues and comply with ISPs. Kirlappos et al. (2015), report that employees' feedback should be taken into account during the ISP creation process, to avoid creating security policies that are cumbersome and overlooked. Sommestad et al. (2014) argue that it is more effective to

encourage employees to participate in the decision process and in the creation of a common vision rather than apply sanctions.

National culture has an impact on ISP compliance. Connolly et al. (2015) found that group non-compliance was more common in collectivistic cultures, such as Ireland, suggesting a need for different security training according to the national culture. Dinev et al. (2009) report that in collectivistic cultures (i.e. South Korea), users may be influenced to use protective technologies by the opinions of their superiors and behaviour of others, whereas in individualistic cultures (i.e. the U.S.), peers or leaders do not influence users' intention to use such technologies.

Dinev & Hu (2007) have identified *technology awareness* (individuals' awareness of security issues, of the effectiveness of security tools and of the consequences of not using them) as a factor influencing individuals' intention to use protective technologies such as anti-spyware. This study suggests that security managers should not only guide employees on how to use protective technologies but also inform them of the consequences of not using them. *Perceived ease of use* and *perceived usefulness* (individuals' perceptions about being more productive if they use antispyware, as their computers are more efficient without the spyware) have an impact on the intention to use protective technologies. Herath et al. (2014), also report perceived ease of use and perceived usefulness to be factors determining individuals' attitude towards using an email authentication service. They also point out that usability which is expressed through *perceived responsiveness* (individuals' perceptions about the time that takes for a security tool to respond) played a role in forming users' perceptions about its ease of use which in turn influenced their security behaviour.

2.2.2 Findings

After analysing relevant literature, mainly deriving from questionnaire-based surveys to identify various factors determining security behaviour, it was found that some factors have conflicting results e.g. sanctions, perceived severity of sanctions (or punishment severity or deterrent severity), perceived certainty of sanctions (or deterrent certainty or detection certainty), rewards, self-efficacy, perceived organisational support. Furthermore, it was identified that different terms refer to similar concepts (in the case of perceived certainty of sanctions, deterrent certainty and detection certainty, in the case of perceived severity of sanctions, punishment severity and deterrent severity, in the case of response efficacy, perceived effectiveness of one's actions and perceived security protection mechanisms, in the

case of perceived value congruence and organisational commitment). There is confusing terminology which is difficult for security managers to comprehend if they are unfamiliar with relevant literature and theories (including for example terms such as perceived value congruence, preconventional moral reasoning, response efficacy, threat appraisal and coping appraisal). It was found that there is no single compilation of all the different factors influencing ISP compliance because each individual paper focuses on specific aspects related to the theory that is being applied. There is limited guidance on how these factors can be exploited in a practical way by security managers in order to enhance ISP compliance.

Finally, while there are some factors relevant to technology in the literature on security behaviour, these are limited in number, e.g. perceived ease of use, perceived usefulness and perceived responsiveness and do not analyse in much detail the role of technology in influencing security behaviour. As a result, it was found that there is a need to delve into more detail concerning security technologies, in particular regarding the perceptions of users, to gain more insights into how security tools and technology can shape security behaviour. While literature provides a wealth of information for security management to assimilate and act on, there is a clear need for clarification, a need to make this complex field more accessible and user-friendly for security management and further elaboration on the implications of these factors if the findings of current literature are to be fully and readily exploited by security management.

2.3 The role of technology

Several studies in the field of Human Computer Interaction (HCI) exploring the usability of tools and technologies draw on usability characteristics as defined in ISO/IEC 9241-11:1998 (ISO/IEC 9241-11:1998, 1998), namely *effectiveness* (the degree of accuracy and completeness with which the user accomplishes tasks successfully), *efficiency* (resources, often referring to time, that are required by the user to accomplish tasks) and *satisfaction* (users' positive attitudes towards the use of a tool).

Nielsen (1994) uses the concept of *efficiency,* described as *efficiency to use,* and employs the term *errors* instead of *effectiveness*, *learnability* (the degree to which a particular user who has never seen the user interface before can learn how to accomplish basic tasks) and *memorability*. Nielsen also provides a list of usability heuristics which technologies should integrate (Nielsen, 1994; Nielsen, 2005), identifying *visibility of system status* (users being kept aware of the system and its functions by receiving feedback), *match between system and the real world* (the system should use the language, terms and concepts that users are aware of),

user control and freedom (users should be able to undo their actions), *consistency and standards* (one action should have the same result and same format to help users recognise them), *error prevention* (the tool informs users about potential errors and tries to inform them by displaying a message that asks for users' confirmation before proceeding)*, aesthetic and minimalistic design* and *help and documentation.* These heuristics have significantly influenced relevant research, such as Seffah et al. (2006), who developed a model for usability measurement which further includes *accessibility, trustfulness* etc. Relative research in the field of usability of security and privacy tools also draws on these characteristics, modifying them accordingly. Johnston et al. (2003) use some of Nielsen's characteristics to develop their own criteria for developing usable and secure interfaces, including *visibility of system status*, *aesthetic and minimalistic design* and *satisfaction*. Johnston et al. (2003), introduced a new usability aspect, namely *convey features* which is the degree to which the tool helps the user understand the security features the tool supports. They used the above usability characteristics to evaluate the Internet Connection Firewall (ICF) of Windows XP suggesting an improved version, concluding that any security interface can be easily improved if usability characteristics are applied.

Furnell (2010) suggests that usable security tools need to support *visibility.* In contrast to the idea of *aesthetic and minimalistic design*, where the tool displays only the most relevant security related information, Furnell (2010) uses the case of an antivirus to show that sometimes additional features are incorporated to show users that "something is going on", e.g. a meter or a chart displayed during the scanning process, as a way of reassuring or attracting users (2010). He also proposes a new usability characteristic called *locatability* (the degree to which security features are evident to users who can easily accomplish security tasks without spending too much time looking for security). Dhillon et al., use locatability with a broader meaning using the term ease of system navigation (Dhillon et al., 2016).

Analysing usability of privacy tools, Wästlund et al. (2011), employed similar terms such as *control*, which refers to the control over users' personal data and *transparency*, which is another term for *visibility*, referring to the degree to which users can see the internal operations of tools and know how their data is being processed. *Feedback* in this case, refers to the information they receive about the handling of their data and whether their privacy is protected or not. Furthermore, a recent ENISA report (Enisa report, 2016) introduced new usability characteristics relevant to the installation process including *ease of installation, registration with personal data, changes upon registration, minimum requirements.* In their report they also referred to the *available help and support.*

A limited stream of research studies users' attitudes and perceptions with regard to the usability of technologies such as e-banking authentication systems (Weir et al., 2009), email authentication services (Herath et al., 2014), antispyware and encryption tools (Dinev & Hu, 2007) and Android pattern lock screens (Andriotis et al., 2016). Weir et al., asked users to use three different e-banking authentication mechanisms to measure their *effectiveness*, *efficiency* and *satisfaction* (Weir et al., 2009), concluding that users have' different usability preferences for different mechanisms, e.g. users preferred the more efficient push button token (which required less steps for authentication compared to the other two mechanisms), but they regarded chip and PIN-Secured tokens as more secure. Similar findings were reported in the study by Krol et al., (2015) where participants also preferred authentication mechanisms that were faster and required fewer steps. This study also found that users were confused when authentication in different e-banking systems included different terms (e.g. "password", "passphrase", "user ID") for similar concepts (Krol et al., 2015).

Whitten and Tygar (1999) found that PGP users had difficulties in terms of *efficiency* and *effectiveness of the tool*, as they were unable to complete all tasks successfully in a timely manner. This could be attributed to security limitations of the interface, such as the display of confusing images for the keys, the fact that users might mistakenly delete their key and be unable to retrieve it (irreversible actions). According to them, users also encountered *understandability* problems. In another study where the usability of Tor interfaces was examined, *understandability* was also studied described as *users being aware of the tasks they must perform* (Clark et al., 2007). In Weir et al. (2009), this usability characteristic was defined as *know what to do next*, with a slightly different meaning, referring in this case to the degree to which users knew how to generate the random number from the e-banking authentication mechanisms and apply it on the website for authentication. Efficiency problems are also reported by Herath et al., (2014), where responsiveness is also introduced as a usability characteristic referring to how much time the system takes to respond. In the case of an email authentication service, users form negative views of the tools' ease of use if it takes too long to indicate whether emails were sent from an authenticated entity. Finally, Lee and Kozar (2005) studied factors that influence users' adoption of an antispyware tool and identified that *computer capacity* had a significant positive influence on users' adoption of the tool

2.3.1 Findings

While literature provides a wealth of information of the usability characteristics for security and privacy tools, review of this research reveals a number of challenges for security

management. Firstly, there is no single study that encompasses all the usability factors for security and privacy tools. Secondly, the majority of these characteristics are not empirically tested with the result that the significance of these factors is not evidenced. Furthermore, some of the factors uncovered in this review can refer to overlapping concepts, e.g. visibility and feedback, which creates confusion for security managers when deciding which security to implement. Finally, users' views regarding which usability factors they consider as important are scarcely addressed.

2.4 Conclusions of the analysis of related research

The first research objective of this Thesis is to identify the factors that influence security behaviour. The review of current literature, on security behaviour and usability presented in this Section identifies a plethora of security behaviour determinants that influence security behaviour, which can further be grouped into three main categories:, organisational, individual and technological.

The second research objective is to explore how these factors can be exploited to develop enhanced security management practices. Study of relevant literature reveals many valuable insights, yet often there are conflicting findings as in the case of sanctions for instance, as well as confusion regarding the content of the concepts and the terms used, with some factors having similar meanings different names, such as Punishment Severity (or Perceived severity of sanctions or deterrent severity). As a result, there is a need for further clarification to enable security management to benefit and exploit the literature to enhance ISP compliance. Moreover, given the complexity and range/diversity of security behaviour factors, it emerges as a necessity to compile and classify the factors into a more accessible and user-friendly roadmap for security management, whereby security managers would be able to understand and clearly identify the most important aspects of security behaviour.

This review also highlights the fact that technological factors are not adequately studied, especially in terms of users' perceptions. There is not a concise compilation of the different usability characteristics to facilitate a clear understanding and comprehensive view of all the different usability characteristics. There are overlapping concepts and some of the usability characteristics are not empirically tested; for these reasons we conducted further research to gain a better understanding of the usability factors that influence users' security behaviour.

Factors identified	Description	Relevant studies
Threat appraisal (or Security breach Concern level)	Individuals' perceptions of possible threats and their severity.	(Herath & Rao, 2009a), (Siponen et al., 2006)
Perceived Severity (or Perceived Severity of Security Breach)	individuals' perceptions about the severity of security threats	(Herath & Rao, 2009a), (Pahnila et al., 2013), (Siponen et al., 2014), (Vance et al., 2012)
Perceived Vulnerability (or Perceived Probability of Security Breach)	individuals' perceptions of vulnerabilities and threats	(Pahnila et al., 2013), (Siponen et al., 2014), (Vance et al., 2012), (Ifinedo, 2012)
Coping Appraisal	individuals' perceptions concerning their competence in complying with ISPs and the effectiveness of ISPs	Siponen et al. (2014)
Self-efficacy	individuals' perceptions of how capable they are of following ISPs	(Herath & Rao, 2009a), (Siponen et al., 2014) (Siponen et al., 2006), (Vance et al., 2012), (Ifinedo, 2012)
Response efficacy	individuals' perceptions of whether ISPs are effective in preventing security threats and of whether individuals' security actions can benefit the organisation	(Pahnila et al., 2013), (Vance et al., 2012), (Ifinedo, 2012), (Siponen et al., 2006)
Response efficacy (or Perceived Effectiveness)	individuals' perceptions of whether of whether individuals' actions can benefit the organisation if they comply with the ISPs	(Herath & Rao, 2009a),
Response efficacy (or Perceived Security Protection mechanisms)	individuals' perceptions of whether security tools are effective in preventing security threats.	(Zhang et al., 2007)
Response cost (or Cost of compliance)	Individuals' perceptions of the possible negative consequences, such as	(Herath & Rao, 2009a), (Vance et al., 2012), (Bulgurcu et al., 2010)

	inconvenience, additional effort and time, that derive from ISP compliance.	
Information Security Awareness	Individuals' knowledge of information security and of the specific ISP of the organization.	(Bulgurcu et al., 2010)
General Information Security Awareness	Individuals' knowledge of information security.	(Bulgurcu et al., 2010)
ISP Awareness	Individuals' knowledge of the content of specific ISPs.	(Bulgurcu et al., 2010) (Pahnila et al., 2013)
Awareness of SETA programs	Individuals' knowledge of Security Awareness and Training Programs.	(Bulgurcu et al., 2010), (D'Arcy et al., 2009)
Awareness of monitoring mechanisms	Individuals' knowledge of the monitoring mechanisms in place.	(D'Arcy et al., 2009)
Habits	Individuals' actions conducted unconsciously.	(Pahnila et al., 2007), (Vance et al., 2012)
Rewards	Possible rewards include pay raises, personal mention, promotions, etc.	(Bulgurcu et al., 2010), (Vance et al., 2012)
Sanctions	Penalties, such as fines, following non-compliance.	(Bulgurcu et al., 2010)
Punishment Severity (or Perceived severity of sanctions or deterrent severity)	Individuals' perceptions about the severe punishment they will receive for violating ISPs	(Herath & Rao, 2009a), (Herath & Rao, 2009b), (D'Arcy et al., 2009), (Son 2011)
Detection Certainty (or Perceived Certainty of Sanctions or deterrent certainty)	Individuals' perceptions about the possibility of getting punished for violating ISPs	(Herath & Rao, 2009a), (Herath & Rao, 2009b), (D'Arcy et al., 2009), (Son 2011)
Preconventional moral reasoning	Individuals' perceptions and fear about the punishment they will receive if they do not follow ISPs	(Myyry et al., 2009)
Openness to change	The extent to which individuals follow their own interests and goals	(Myyry et al., 2009)
Threat to freedom	The extent to which individuals believe that their freedom is threatened by ISPs	(Myyry et al., 2009)

Reactance proneness	The extent to which individuals react when they believe that their freedom is restricted by ISPs	(Myyry et al., 2009)
Privacy concerns	Individuals' perceptions about their privacy	(Herath et al., 2014)
Perceived Cost of Noncompliance	Sanctions, negative feelings and vulnerability of resources connected to failure to comply with the ISPs.	(Bulgurcu et al., 2010)
Perceived Benefit of Compliance	Positive feelings, rewards and decreased vulnerability in resources that result from compliance with the ISPs.	(Bulgurcu et al., 2010)
Perceived Legitimacy	Individuals' perceptions concerning how fair or just ISPs are	(Son, 2011)
Perceived Value Congruence	the degree to which employees' own values match those of their superiors	(Son, 2011)
Age	Individuals' age	(Pahnila et al., 2013)
Gender	Individuals' gender	(Herath & Rao, 2009b)
Top management participation	Individuals' perceptions that top management is actively involved in security practices by following them	(Hu et al., 2012)
Information Quality	Users' perceived quality of the information included in the ISPs.	(Pahnila et al., 2013), (Pahnila et al, 2007)
Facilitating conditions (or Resource Availability or Controllability or Visibility)	Resources provided to facilitate compliance, including encouragement, time, help from experts, access to ISPs, etc.	(Herath & Rao, 2009a), (Pahnila et al., 2007), (Siponen et al., 2006)
Visibility	information relevant to IS security, that is available to the organisation through inside and outside sources	Siponen et al. (2006)
Organisational commitment	The degree to which users share organizational goals.	(Herath & Rao, 2009a)

Subjective norms (or Normative beliefs)	Individuals' perceptions of significant others' expectations e.g. colleagues, superiors, etc.	(Herath & Rao, 2009a), (Siponen et al., 2006), (Pahnila et al., 2007), (Herath & Rao, 2009b), (Siponen et al., 2014), (Ifinedo, 2012)
Descriptive norms (or Peer behaviour)	Individuals' perceptions of significant others' behaviour	(Herath & Rao, 2009a), (Herath & Rao, 2009b)
Involvement	Individuals' participation in meetings and relationships with colleagues who share the same security views	(Ifinedo, 2014)
Commitment	The degree to which individuals are focused on acquiring high quality job	(Safa et al., 2016)
Knowledge sharing	Individuals' sharing of information security knowledge with their colleagues	(Safa et al., 2016)
Collaboration	Individuals' communication with IT experts in order to inform them about security breaches	(Safa et al., 2016)
Intervention	Individuals' participation in different training programs, e.g. seminars, receiving newsletters, etc.	(Safa et al., 2016)
Experience	Individuals' experience about information security	(Safa et al., 2016)
Job satisfaction	Individuals' satisfaction of their job	(D'Arcy and Greene, 2014)
Perceived organisational support	Individuals' perceptions that the organisation values their contribution and is concerned about their well-being	(D'Arcy and Greene, 2014)
Organisational culture	Individuals' behaviour based on the organisational culture	(Connolly et al., 2015)
National culture	Individuals' behaviour based on their national culture	(Connolly et al., 2015), (Dinev et al., 2009)
Technology Awareness	Individuals' awareness of security issues, of the effectiveness of security	(Dinev & Hu, 2007)

	tools and of the consequences of not using them	
Perceived Ease of Use	Individuals' perceptions of how easy a security technology is.	(Dinev & Hu, 2007)
Perceived Usefulness	Individuals' perceptions of whether a security technology will make their computers more efficient or whether a security technology will thwart the security threats and risks.	(Dinev & Hu, 2007), (Herath et al., 2014)
Perceived Responsiveness	Individuals' perceptions about the time that takes for a security tool to respond	(Herath et al., 2014)
Easy installation	Security tools are easy to install	(Enisa Report, 2016)
Avoid registering for ease of use	Users do not register with their personal data to use security tools for ease of use	(Enisa Report, 2016)
Changes upon installation	There are minor changes upon installation	(Enisa Report, 2016)
Minimum requirements	Minimum requirements needed for installation are clearly indicated	(Enisa Report, 2016)
Available information and support	There is access to information and support	(Enisa Report, 2016), (Nielsen, 2005)
Language	Language of security tools does not include many technical terms	(Nielsen, 2005)
Locatability	Security settings are easy to find	(Furnell, 2010), (Weir et al., 2009)
Understandability	Users know how to perform security tasks	(Furnell, 2010), (Whitten & Tygar, 1999), (Weir et al., 2009), (Clark, 2007)
Feedback	There is feedback to inform users about their actions	(Nielsen, 2005)
Visibility	Here are status indicators, pictures, etc to show users what is happening inside the tools in terms of security	(Johnston et al., 2001), (Furnell, 2010) (Nielsen, 2005)
Undo	Users are able to undo their actions	(Nielsen, 2005)

Error prevention	Users are informed on how to avoid potential errors	(Nielsen, 2005)
Control	Users have control over the security tools	(Nielsen, 2005)
Learnability	Users can easily learn how to use the tool	(Nielsen, 1994)
Satisfaction	Users are satisfied when using the security tool	(Weir et al., 2009), (Nielsen, 1994)
Effectiveness	Users can complete the tasks and use the security tools successfully	(Weir et al., 2009), (Nielsen, 1994)
Efficiency	Security tools are efficient	(Weir et al., 2009), (Nielsen, 1994) (ISO 9241-11, 1998)
Aesthetic and Minimalistic Design	Security tools have a minimalistic design and follow modern design standards	(Nielsen, 2005)
Accessibility	Security tools are accessible for people with disabilities	(Seffah, 2006)
Consistency	There is consistency in format among security tools	(Nielsen, 2005)
Control of personal's data	Users can control their personal data when using security and privacy tools.	(Wästlund et al., 2011)
Transparency	There is transparency with user's personal data in security and privacy tools.	(Wästlund et al., 2011)

Table 2: Factors influencing security behaviour

Chapter 3: Research Outline

3.1 Introduction

This Thesis has two research goals: to identify factors that influence information security behaviour and to use this information to enhance information security management practices. These two goals are closely connected since in order to improve a situation it must first be understood fully before any problems can be addressed. Thus, to enhance current security management it was first essential to analyse all the factors involved in security behaviour and explore their role identifying how current security management practices adopt or fail to adopt them. In the following, we provide guidelines on how to exploit this knowledge in order to enhance current practices.

3.2 Stages of research

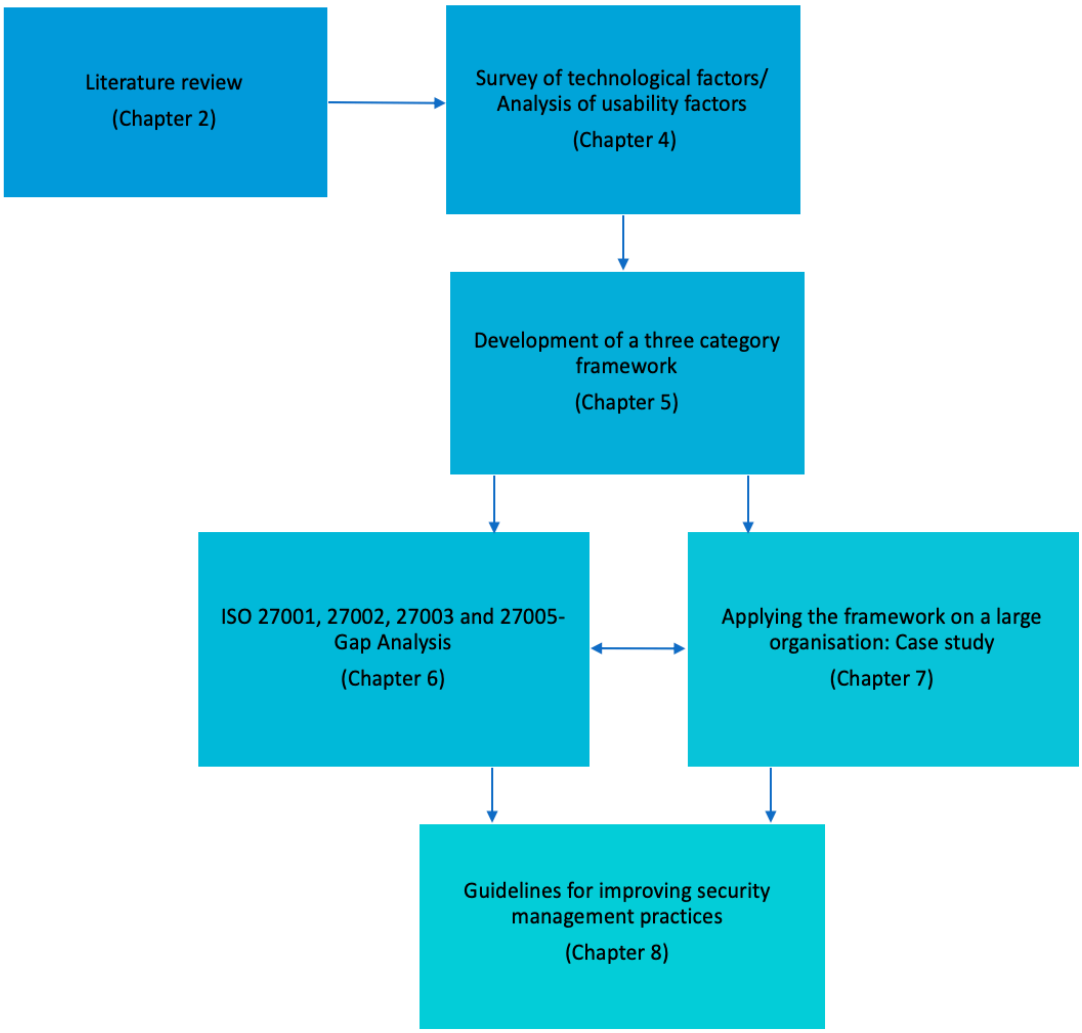

Figure 1: Stages of the Research Design

The first aim of this research is to identify all the factors involved in employee security behaviour. This required a thorough and comprehensive review of current literature in this field, achieved by collecting data from search engines and from references of papers with a significant number of citations. In total, 28 studies on factors influencing security behaviour were identified, through search engines such as Google Scholar and Scopus, using the following keywords: “ISP compliance”, “employees’ compliance with security policies”, “security behavio(u)r”, “factors influencing ISP compliance” and “factors influencing security behavio(u)r”. Some studies derived from the references list of the manually identified papers. Analysis of the literature generated an extensive list of factors influencing security behaviour but also led to two significant conclusions:

First, while the role of technology in shaping security behaviour is identified, the literature on this field lacks adequate analysis of the technological factors influencing security behaviour. Therefore, further investigation of this role was the next step and this was done by conducting a survey on the usability characteristics of security and privacy tools.

A survey consisting of a questionnaire and individual follow-up in-person interviews was chosen to gain insights into users’ views when using such tools. According to literature, interviews facilitate the study of individual behaviour since the interviewees can describe their experiences and incidents (Maykut & Morehouse, 1994). The first stage involved creating the questionnaires based on usability characteristics previously identified in literature. After selection of three tools-namely, Malwarebytes, Ghostery and Tor, followed a cognitive walkthrough and the development of three scenarios to involve core tasks of the tools which were mapped to usability characteristics. This then led to the design of one questionnaire for each tool to ascertain users’ views on its usability. Before conducting the actual survey, a pilot test was carried out with two students resulting in some minor revisions to the questionnaires based on their comments.

For practical reasons it was not feasible to obtain feedback from a large sample of individuals. In order to ensure a sizeable number of responses, the survey enlisted the participation of 150 3rd year ICT students. This selection of knowledgeable ICT students may also have yielded more detailed responses and led to more insights into the design of security and privacy tools in terms of usability.

All 150 participants were asked to install and use the tools on their own computers, unobserved, follow the scenarios and complete the questionnaires online. Participants were asked to keep notes of the steps they followed and produce a report describing the tasks they

carried out, including the appropriate print screens of their actions. Subsequently, there were follow-up interviews to further determine users' attitudes to the tools regarding their usability.

The second important conclusion deriving from the analysis of literature on security behaviour was that the quantity of academic research in this domain and the complexity of the theories involved would be extremely challenging for any information security manager to cope with. As a result, there is a need for a more clear, concise and more comprehensible approach so that results of this wide body of academic research becomes accessible and applicable to information security management.

Three major categories of factors emerged from the analysis of current literature and the usability survey of security and privacy tools: individual, organisational and technological. Given the vast number of different factors generated by the review of current literature, as well as their complexity and sometimes confusing and overlapping terminology, a framework was developed using the above-mentioned main categories adding sub-categories of grouped factors expressed in terms that would be more comprehensible to information security managers and relevant to their practices.

Moving from theory to practice, in order to better understand actual security management practices, the next phase involved analysing security management standards, in particular the ISO Standards (ISO 27001, 27002, 27003 and ISO 27005). A gap analysis of these standards against the set of factors included in the Technological-Organisational-Individual framework highlighted that several findings and a considerable amount of the accumulated knowledge on security behavior are either not included or not adequately addressed.

In addition to using the framework to analyse current standards, this framework was also applied in practice to analyse security management practices in a real organisation. Literature provides insights on how case studies can be conducted (Yin, 2011; Western Sydney University, 2016). This case study mapped the factors listed in the framework against the current practices of the organisation. The case study also yielded interesting insights concerning practices that are neither mentioned in ISO nor in relevant literature.

In line with the second research aim of this Thesis, namely to exploit academic knowledge on security behavior for enhancing security management, the Thesis drew on findings from each previous stage of the research process to produce a collection of guidelines for information security managers. The purpose of this last phase was to offer security managers a concise set of guidelines covering all the essential areas and points they need to consider, including additional practices, in order to enhance security management practices and consequently improve ISP compliance among employees.

3.3 Conclusions

In this chapter, the research outline of this PhD Thesis is presented. Different research methods, including walkthroughs, scenarios, questionnaires and interviews were employed to support the research questions of this PhD Thesis. After thorough analysis of the literature to identify which factors influence security behaviour and a survey conducted through questionnaires and interviews, it was possible to determine a plethora of security behaviour determinants. Then a framework was derived, which was mapped against security management practices provisioned by ISO/IEC Standards and followed in a real life organisation. Finally, recommendations to security management are provided to serve as a roadmap for security managers in order to enhance their practices and lead to improved ISP compliance.

Chapter 4: Exploring the role of Technology in security behaviour: Usability factors

4.1 Introduction

In Chapter 2 a literature review was conducted in the field of security behaviour. Through this analysis it was identified that the role of technology has an impact on security behaviour (Dinev & Hu, 2007; Herath et al., 2014). To investigate further the role of technology and which characteristics influence uses to use security and privacy tools, relevant literature was investigated and a set of usability characteristics of security and privacy tools was identified (section 2.4).

To further explore the technological aspects and in particular users' perceptions about the usability of security tools, a usability survey was conducted. The tools that were selected for this survey include both security and privacy tools. The security tool, Malwarebytes is a popular antimalware tool, selected due to the severe impact of ransomware malware such as "Wannacry" (Symantec, 2017) and "Petya" (TechCrunch, 2019). The privacy tools, namely Ghostery (anti-tracking tool) and Tor (anonymising network), were selected as representative from the list of tools included in the (Enisa Report, 2016).

While, ideally, this survey should have been carried out on employees to assess their usability views about which usability characteristics they regard as important, was not feasible for practical reasons. Thus, the survey was carried out among ICT students and a large number of 150 participants was the final sample of this survey. Since they were more knowledgeable about ICT tools deeper insights were gained into the design of the tools in terms of usability that might otherwise not have been revealed.

As the new trend in organisations is teleworking and working in an environment different from the conventional office, the survey was not conducted in the lab. Participants were not observed when using the tools or filling in the questionnaires. This was considered an effective way to simulate modern working conditions and participants were asked to provide their views after using the tools.

This survey investigates a broad spectrum of usability characteristics including factors relevant to installation. This was due to the fact that it is very common for employees who are using laptops or their own devices following the "Bring your own device" (BYOD) practice. These employees have the flexibility to install software depending on their needs. In the case of BYOD, where users use their own devices, they are responsible for installing the appropriate security tools and setting up the security settings themselves. Furthermore, usability

characteristics relevant to privacy tools were also assessed by users. This was due to the fact that some employees might be working on highly confidential positions e.g. in organisations that are handling confidential information, e.g. nuclear factory, bank, etc. and they need to ensure that their privacy and anonymity are protected. Privacy was also investigated since some employees might be privacy conscious and they want to install and use privacy tools in their computers.

4.2 Data collection

Drawing on the analysis of relevant research we identified a comprehensive set of usability characteristics (described in the following section) and designed three different scenarios that involved using three commonly used tools, namely Malwarebytes, Tor and Ghostery. Through cognitive walkthrough of the tools' functionality, suitable scenarios were developed including core security tasks. Participants of this survey were third year ICT university students, their age ranging from 20 to 25 years old. Participants were asked to install the tools on their personal computers unobserved, and follow the required security tasks, which were described in scenarios. After completing the scenarios, students filled an online questionnaire of 40 questions, providing their views on certain usability characteristics. Prior to providing students with the questionnaires, a pilot study of the first scenario with two individuals was performed. The questionnaires also included open questions in order to receive more feedback on users' actions when completing the tasks, their understanding of how the tools work and their views regarding the tools' usability. Overall, there were gathered 150 completed questionnaires, between March and April 2017. 65% of respondents were male.

Follow-up interviews with 112 respondents lasting approximately 15 minutes were conducted, to further explore users' views and expectations with regard to the usability of security and privacy tools. The questions focused on the effectiveness of the tools used, their positive/negative aspects, the time spent carrying out the set tasks, whether they would use the tools in the future and what changes, if any, they would make if they were to design the tools.

4.3 Scenarios' description

Three scenarios were developed including tasks which were linked to the usability characteristics identified through the literature review in section 2.4. The steps of the scenarios

are included in more detail in Annex 1 of this Thesis. Below there is a brief description of each scenario.

In scenario 1, users' tasks were to: download and install the English version of Ghostery; create an account and register with personal data; block and restrict different types of trackers on specific websites; block slow trackers on one website; configure the position of the purple box and its duration on their screen; select the option "block every new tracker by default" and undo the blocked and restricted trackers from all the previously visited websites.

In scenario 2, users' tasks were required to: download and install the English version of Malwarebytes; select the option "scan for rootkits"; carry out a threat scan and delete any malware that was identified; select all the available disks and "scan for rootkits"; conduct a custom scan; save and read the reports of the scanning processes.

Finally, scenario 3, users' tasks were to: download and install the English version of Tor; test the security settings of Tor; use the appropriate search engine; check that https is enabled; set security level to high; visit a designated website and change the settings to view its content (by minimising the security level and temporarily allowing the scripts); maximise security level and revoke the permissions; visit a designated website, globally allow the scripts to view one video that was not available and then revoke permissions; visit another specified website which does not support SSL encryption and check if the connection is secure; maximise the browser window and finally create a new identity.

4.4 Results of the Questionnaires' Analysis

In this section follow the comprehensive findings of the analysis of the questionnaires as well as the interviews, with regard to the usability aspects identified in the literature review (section 2.4). Usability characteristics of security and privacy tools that were identified in literature are presented under the relevant headings:

4.4.1 Usability characteristics relevant to installation

With regard to the installation process, 121 out of 150 respondents find it "important or very important" that security tools have an easy installation process. More than three quarters of Ghostery users find it "important or very important" to avoid registering for ease of use, while two users commented that registration was *"unnecessary"* or a *"disadvantage"*. Many Ghostery users had a positive attitude towards the minor change that took place upon

installation, namely the add-on on the browser toolbar. Most users reported that the minimum requirements required for the installation of each tool were clearly stated in all three cases.

4.4.2 Available information and support

In total, 137 users reported that it was "important or very important" for them to have access to available information to guide them on how to use the tool. During the interviews, users reported using a variety of different methods, including the manual, videos/tutorials, FAQs, etc. Users of Ghostery, in particular reported using the quick tour, FAQs and videos in this order of preference, which suggests that they preferred speedy help.

While 106 users out of 111, who used the available help and support, considered the information they received as adequate, there were users who resorted to the Internet for assistance, especially when using Tor. One user felt that the quick tour in Ghostery *"... didn't show all the tool's functionalities"*. In addition, Ghostery and Tor users said that they had expected to find a manual and would prefer a manual that was *"more detailed"*.

4.4.3 Language used

82 users out of 150 reported that they were not concerned about the language and terms used by the tools, despite the fact that they were using the English version, which was not their native language. However, during the interviews some users had difficulty to distinguish between certain terms, namely "block" and "restrict" (scenario 1), "threat scan" and "custom scan" (scenario 2) and "temporarily allow scripts" and "globally allow scripts" (scenario 3). In all three scenarios, many users who had previously claimed to understand the differences failed to explain them correctly.

Thus, it seems that even experienced users are often confused with the terminology. Though one user commented that the *"complexity of the terms block and restrict might confuse novice users",* in fact several respondents found the differences hard to explain, with another user attributing this difficulty to *"the lack of a concise and exact description".* Thus, users may find it difficult to fully comprehend specific terms, especially if they are not in their native language*". It was also identified that* the lack of consistency in similar terms used by different tools can confuse users (e.g. Malwarebytes uses "threat scan" and "custom scan", for which, one of the respondents suggested that they should better be named as *"fullscan"* and *"fastscan" respectively).*

4.4.4 Locatability

In total, 144 students replied that it is "important or very important" for them to find what they were looking for easily. During the interviews it was identified that users had difficulties in finding some options. More specifically, the majority of Ghostery users were not able to locate a specific functionality to perform a certain task (clear tracker settings) (Figure 2). To overcome this, most resorted to alternative solutions such as visiting every website separately to undo the restricted trackers. While they did manage to accomplish the task at the end, they did so through a slower and cumbersome process. *"We were looking for an option to undo the restricted trackers collectively, but we didn't find such an option"*.

Furthermore, when using Tor, users reported that they needed a lot of time to find the security slider, suggesting that security settings should be *"more visible (for a novice user)"*. The user can find the security settings of Tor and adjust the security level of the security slider only if he/she clicks on the "onion" picture as shown in Figure 3. While most users would expect that security settings will be in the same location as general settings, they were located on a totally different place at the website. Furthermore, the picture of the "onion" made it difficult for novice users to understand its role.

According to many respondents' comments, it is preferable to have all settings *"gathered together"* in one location. Moreover, with regard to Ghostery, which is an add-on, users feel *"all the procedures should be conducted from the Ghostery window rather than from different websites"*.

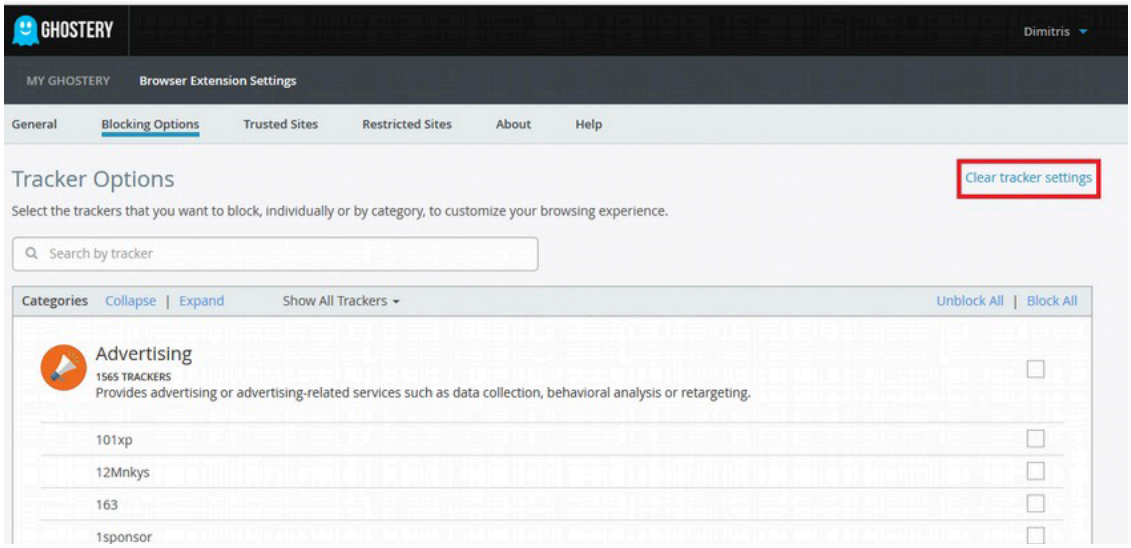

Figure 2: "Clear tracker settings" button of Ghostery

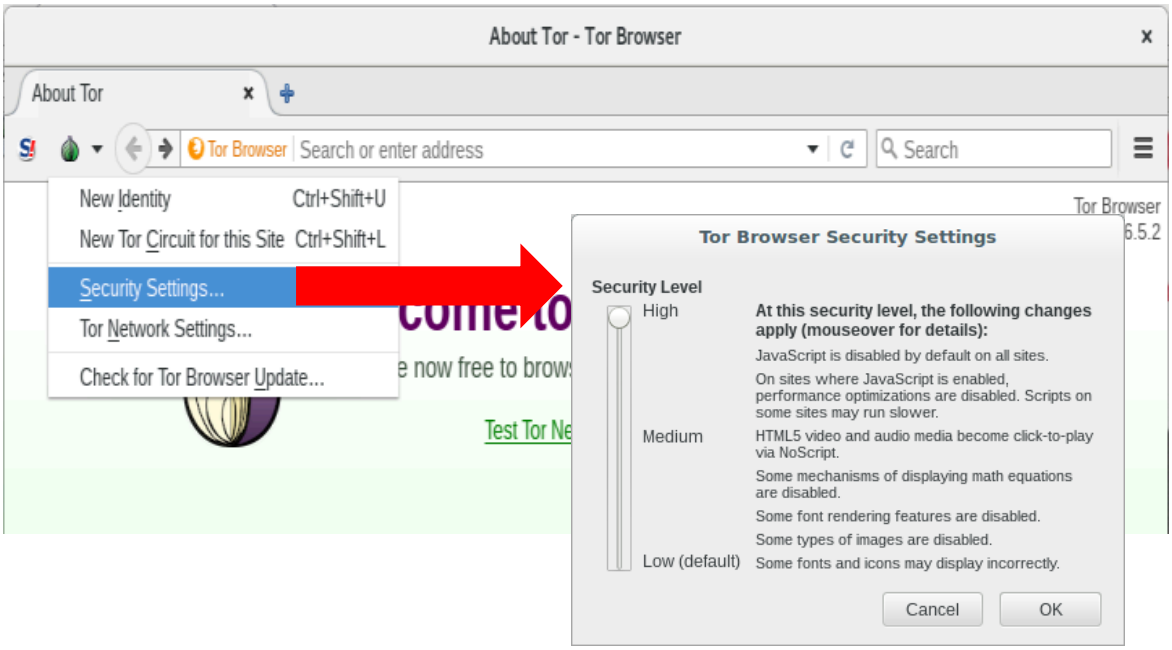

Figure 3: Security slider of Tor

4.4.5 Understandability

125 users out of 150, considered knowing what to do next "important or very important", however, responses during the interviews indicated that they encountered some difficulties.

When using Ghostery, one user reported having difficulty in identifying slow trackers easily as *"there wasn't an "indicative" picture"*. Another user preferred the previous version of Ghostery because *"it was easier to understand and use"*. Another user felt *"lost"* in performing the last 2 tasks and was under the false impression that he had completed the last task successfully, though he had not found the "clear tracker settings" button.

Tor users reported that they found it hard to apply advanced settings such as "set security to high level", "test security settings", "temporarily change settings to view the content of the specific website". One user was unsure what might happen after creating a new identity.

Conversely, all users using Malwarebytes, reported that they knew what to do next and no difficulties were reported. In this case, the tool guided the user through the process, step by step, as after selecting the category of scan and the drives and types of malware to be scanned (in the case of custom scan) the scanning process started automatically. Malwarebytes was intuitive for users and interestingly it was noted that all users competed the tasks of the scenario successfully.

4.4.6 Feedback

A total of 120 users considered receiving feedback as "important or very important". However, most users' responses in all three scenarios indicated that in most cases they did not notice feedback by the tools. One Ghostery user commented that *"a notification that the restriction or blocking of trackers was successful"* would be useful, despite the fact that the tool displayed a similar pop-up message, while some users wanted more feedback *"about each tracker",* and more specifically *"what it is and what it does"*.

Tor users would prefer more and visible feedback *"when the user changes security settings and detailed explanation about their impact"*. Users were not satisfied with the *"small banner"* that appeared when they maximised the window to warn them that this practice is dangerous. Another user would prefer feedback informing him if his browsing *"is not secure"*. When users were asked to perform a search, more than half chose Google Chrome instead of Duck Duck Go, despite the message "Search securely with Duck Duck Go" displayed on the first page of Tor, as shown in Figure 4.

Interestingly, with regard to using Malwarebytes all respondents reported that feedback was noticeable, however a few would prefer to receive more feedback after the scanning process, feeling that the tool did not *"adequately explain what kind of malware is identified"*. It is also important to note that most users did not read the reports provided by the tools, as we found during the interviews.

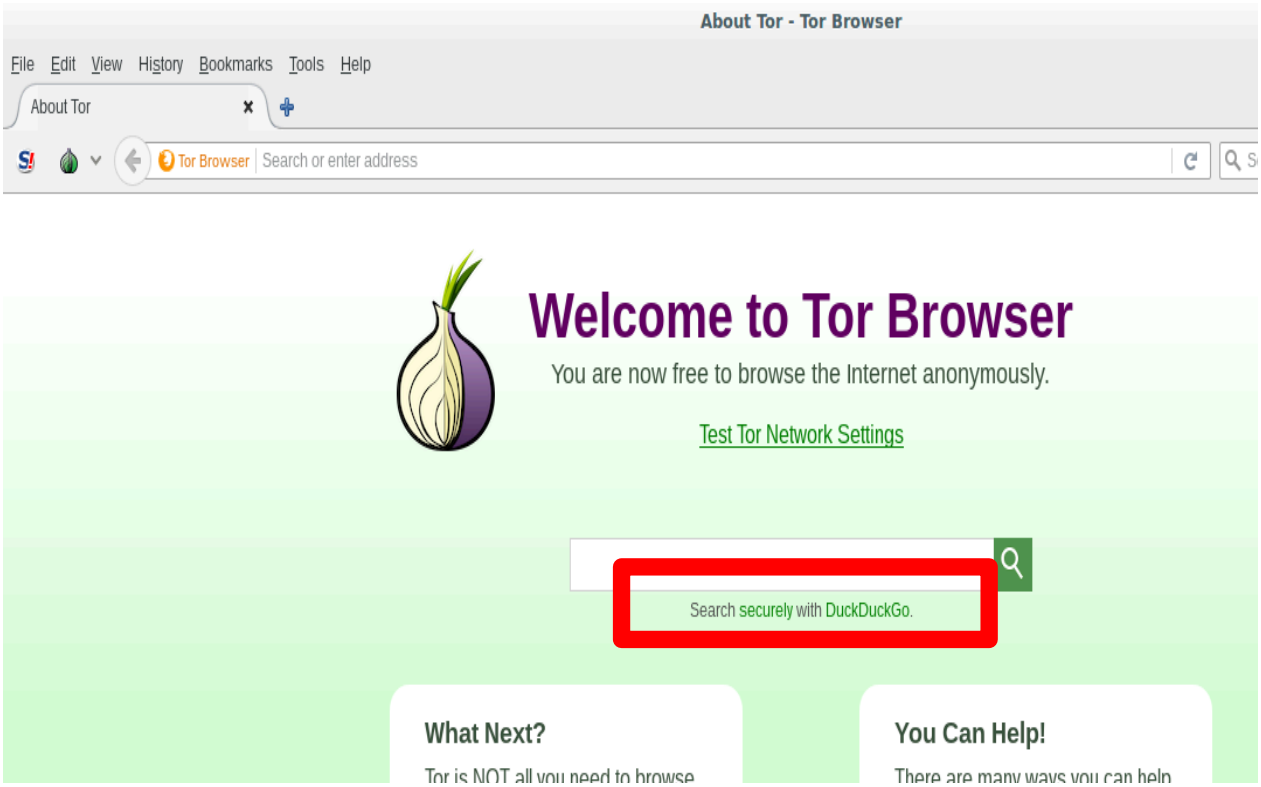

Figure 4: "Test Tor Network Settings" button

4.4.7 Visibility

A total of 110 users regard as “important or very important” the existence of status indicators to show them what is happening inside the tool in terms of security (Malwarebytes) and privacy (Tor and Ghostery). In Ghostery, most users identify as status indicators the use of images of the padlock, the “tick” and the “shield” and their different colours (e.g. red for the padlock and “tick”, green for the shield). One user preferred text to pictures suggesting that *“I would change the buttons block/restrict/trust so that they contain text”*. Interestingly, most users reported that the pie chart displaying the different categories of trackers was a status indicator. However, this is mainly an animation for aesthetic reasons rather than a privacy status indicator.

Generally Malwarebytes, is a tool that has status indicators, for example there is a process diagram that shows live the locations where the tool scans for malware as shown in Figure 5. There is also information about the number of scanned items. Some Malwarebytes users wanted more practical information e.g. *“to see a percentage of scan completion and what has been scanned so far and what is left to be scanned”*.

Most Tor users noticed pictures that indicate the tool’s security and privacy status (e.g. the different pictures of Noscript, the padlock indicating a secure SSL connection, the warning messages). Surprisingly, only a few referred to the security slider as a status indicator, and only two respondents cited the existence of the image that shows the Tor circuit (image showing the path of Tor computers used to hide the user’s IP) (Figure 6). While this Tor circuit is an important indicator of whether Tor is protecting the user’s IP, this is not visible and therefore users do notice it easily. As a result, users’ responses indicate that while there are status indicators in Tor, some of them and especially those which are crucial for ensuring users’ privacy, are not visible and remain unnoticeable.

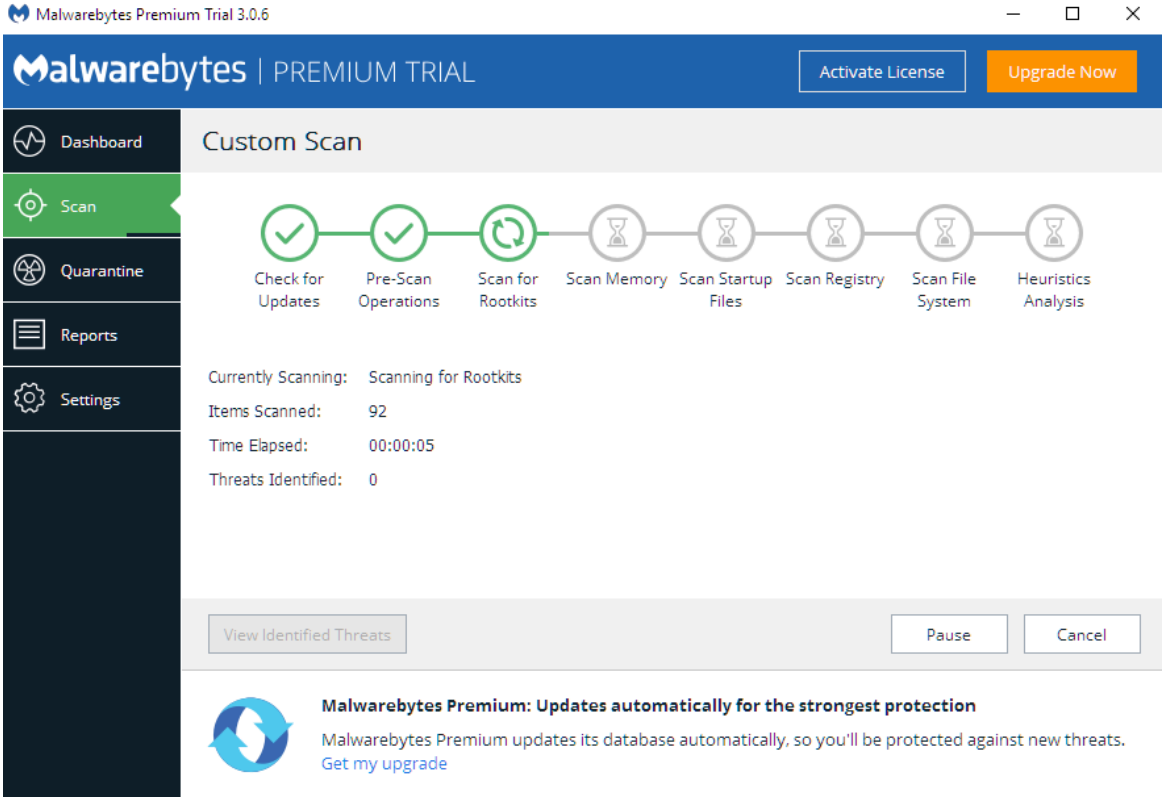

Figure 5: Process diagram showing the status of the scanning process

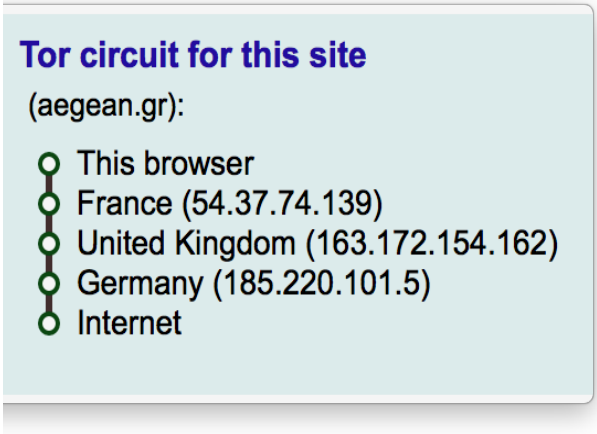

Figure 6: Tor circuit of the nodes used in Tor

4.4.8 Undo

Although in all three scenarios 143 users reported that it was “important or very important” to undo their actions, more than half of Ghostery users were not able to find the

button “clear tracker settings” that would have enabled them to undo the restricted trackers collectively and easily.

4.4.9 Error prevention

The majority of Tor users reported that it is “important or very important” that they receive error messages, displayed as warnings when users apply specific settings, such as maximizing the window and allowing scripts globally.

4.4.10 Control

Although most respondents (142 out of 150) reported that is “important or very important” for them to be in control of the tool they are using, some would prefer Ghostery to provide automated procedures and apply certain settings by default. One user said *“I would prefer it if some procedures were carried out automatically, if the tool blocks some suspicious trackers immediately after installation (by default)”.* Another user further suggested that *“the tool should employ algorithms to block trackers automatically”.*

Malwarebytes users would also prefer some automated procedures to take place. One user reported *“I would automate some updates and threat scans in case users have forgotten”*. While custom scan offers users control by selecting which drives they want to scan, one user would prefer an option to scan everything, *“Threat scan didn’t find one Trojan inside a file in disk “C”. It was found only during custom scan. I would add one option for scanning all the files on my computer, like fullscan”.* Another user was not satisfied with the default settings of Malwarebytes, e.g. *“*Treat as malware” for PUP (Potential Unwanted Program) “*is selected by default […]. This is something that users might not want”.* He also reported that because “Scan for rootkits” is deactivated by default *“users might miss this important option”.*

Tor users were able to control the security level, though they did recognise the trade-off between security and usability, *“When the tool is set to the highest level of security, it hides content from the websites […], the appearance of the website is unattractive”.* As shown in Figure 7 when security slider is set to high, meaning that security protection is high the user cannot view the videos, or any other scripts, since they are automatically deactivated. However, when security slider is set to low, the level of security is low and the user can view all the content of the website (Figure 8).

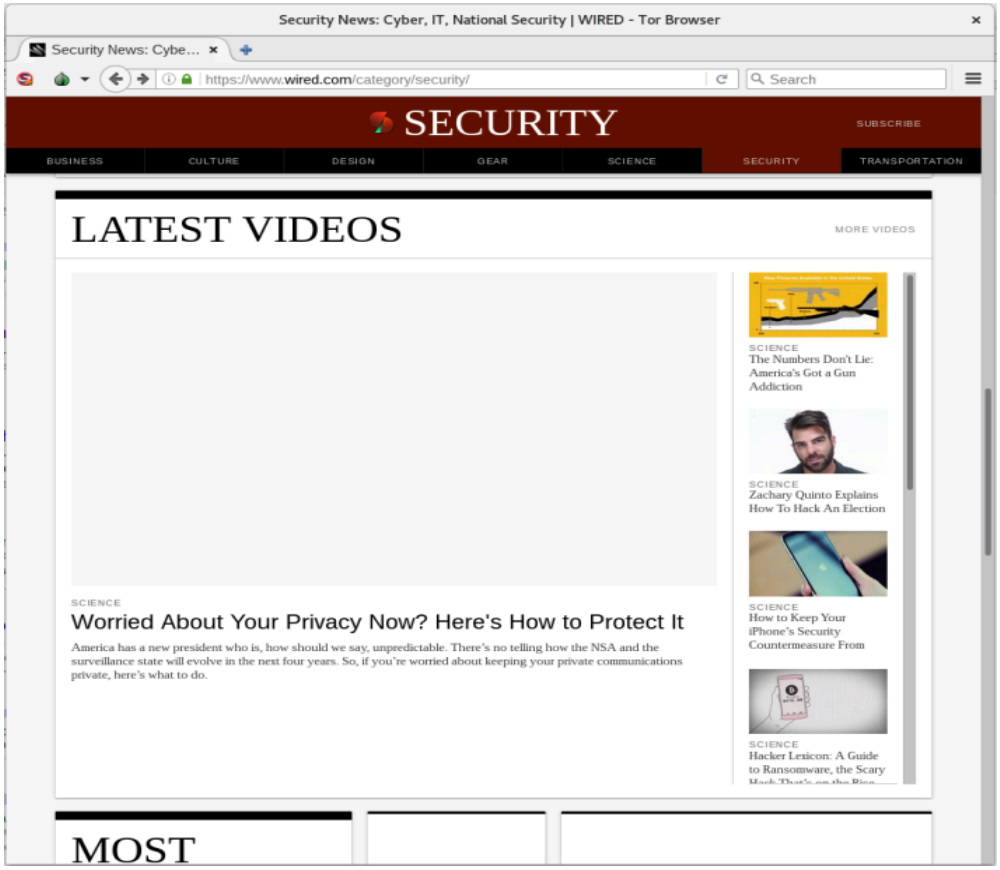

Figure 7: High Security - Low usability

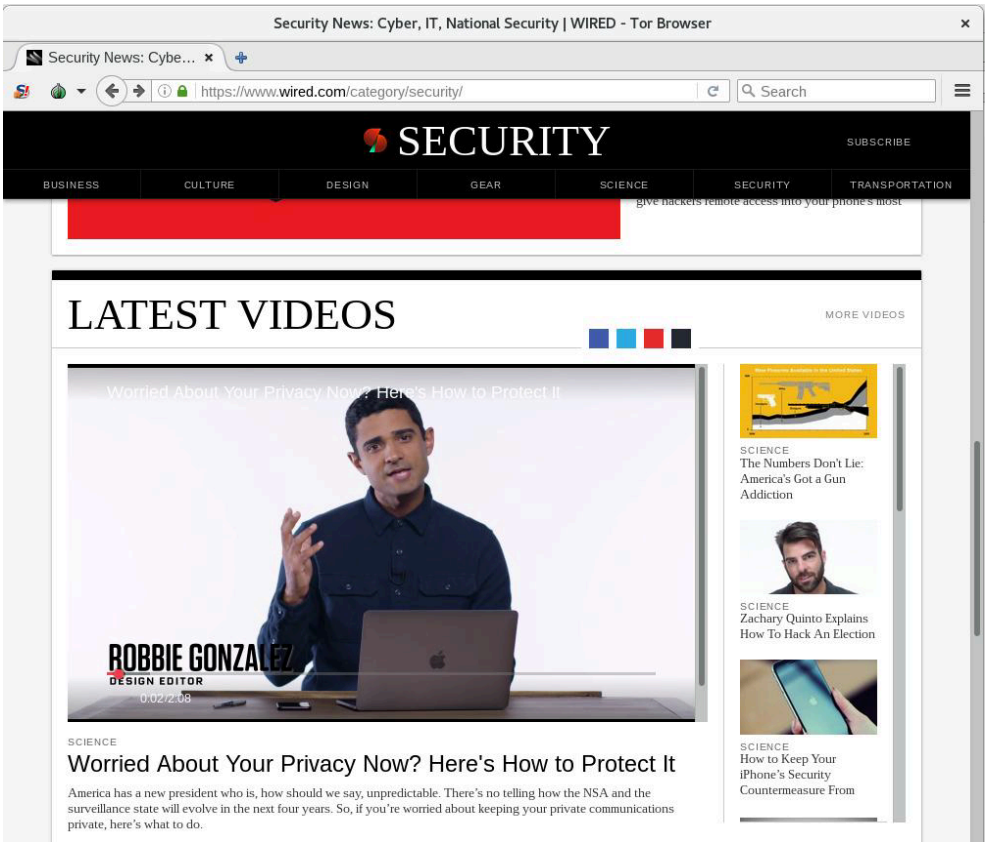

Figure 8: Low Security - High usability

4.4.11 Learnability

The majority of users reported that it was easy to learn how to use the tools.

4.4.12 Satisfaction

While most users were satisfied with all the tools, some users were dissatisfied with Tor, reporting that *"high security settings result in a poorer browsing experience", "being unable to read websites"* or *"having to verify that you are not a robot".*

4.4.13 Effectiveness

While the majority of users stated that tools are usable and easy to use, they were not able to perform some tasks successfully. For example, in Ghostery some users were not able to block some of the specified trackers using Ghostery and many had difficulty in finding the option "clear tracker settings". In Tor, more errors were reported, as some users did not know how to test the settings of Tor, nor understand which settings to configure to view the contents of the website. Many users did not select Duck Duck Go, as a search engine.

4.4.14 Efficiency

In Ghostery some users report that *"there was a considerable delay on the loading of the website when using the tool".* When using Malwarebytes, most users said that custom scan took many hours. This can be attributed to low computer capacity. Furthermore, users reported *"a negative impact on the speed"* of their computers during the scanning process. Tor users reported delays when browsing online with Tor, describing it as *"a slow tool, compared to other browsers. Although it protects users' privacy, it sacrifices browsing speed, which is important for most internet users".* Users want to use security and privacy tools without time delays. Furthermore, for antimalware tools the more computer capacity the better the performance of these tools.

4.4.15 Design and Accessibility

One Ghostery user reported that the purple box (a feature showing all trackers of every website the user visits)(Figure 9) is *"unattractive"*. He further commented that he found it annoying because *"the more trackers there are in one website, the bigger the size of the purple*

box. As a result, it covers the website and the user has less visibility of the website's content. The purple box should be deactivated by default". Users want security and privacy tools to display the appropriate information in a clutter-free way.

Three Tor users were also not satisfied with the design of the interface, commenting that they found it outdated. As one said *"the design components (images, layout of the websites) are not aligned with the modern design trends"*. Another user, however, reported that he was able to use Tor, as it is convenient for color blind people, suggesting that *"Tors' settings are convenient for color blind people like me"*.

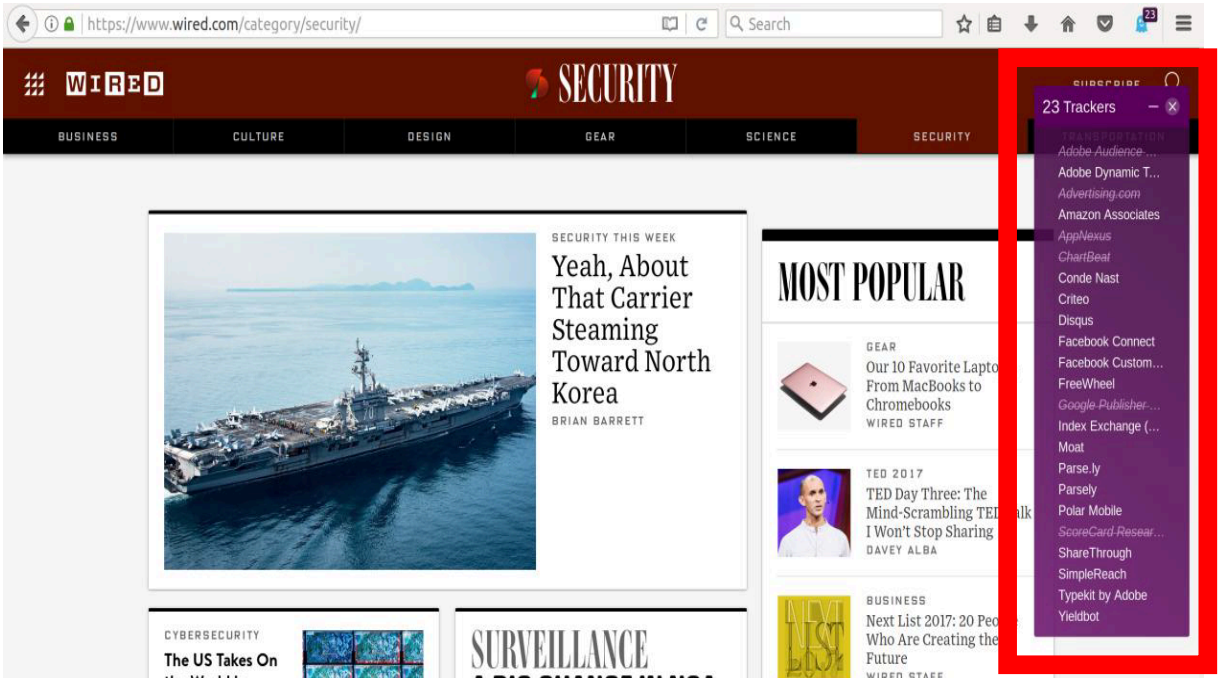

Figure 9: The purple box of Ghostery

4.4.16 Consistency

Users who are accustomed to using tools do not seem to welcome new features easily, e.g. one regular user of Ghostery preferred the previous version without the purple box, which according to his opinion is not usable. This implies that users want design consistency among different versions of security and privacy tools, because otherwise they might be reluctant to use them.

4.4.17 Control of user's personal data and transparency

Some users chose not to share their data with Ghostery. Although this task was not in the scenario, it indicates users' concern about their privacy and their reluctance to share their personal data with the privacy tool company. Respondents expressed their concern about the

lack of *"transparency in the processing of data"* and the possibility that Ghostery might make money from *"selling anonymised data"*. For this reason, some users might be skeptical towards trusting a tool.

4.4.18 Availability of tools among various platforms

Availability of security and privacy tools among different platforms is a usability aspect. In scenario 1, one user wanted to install Ghostery on his smartphone, but *"it was not available"*. In the second scenario, one user reported that *"it was not possible to install Malwarebytes on my computer because I am a Linux user"*.

Usability Factors	Relevant Studies	Users' expectations/views about security and privacy tools - Insights
Easy installation	(Enisa Report, 2016)	Users find it important that tools have an easy installation
Avoid registering for ease of use	(Enisa Report, 2016)	Users find it important if they can avoid registering for ease of use
Changes upon installation	(Enisa Report, 2016)	Users find it important that tools have only little changes upon installation
Minimum requirements	(Enisa Report, 2016)	Users want the tools to indicate the minimum requirements needed for installation
Available information and support	(Enisa Report, 2016), (Nielsen, 2005)	Users find it important to have access to available information and support. Many Ghostery users wanted speedy help. Ghostery and Tor users needed a manual.
Language	(Nielsen, 2005)	Users are not concerned about the number of technical terms used. However, they have difficulties in understanding them.
Locatability	(Furnell, 2010), (Weir et al., 2009)	Users find it important that the tools' security settings are easy to find and they are located in one place.
Understandability	(Furnell, 2010), (Whitten & Tygar,	Users find it important that they know how to perform security tasks.

	1999), (Weir et al., 2009), (Clark, 2007)	
Feedback	(Nielsen, 2005)	Users find it important that tools provide them with detailed and visible feedback.
Visibility	(Johnston et al., 2001), (Furnell, 2010) (Nielsen, 2005)	Users find it important that tools show them what is happening in terms of security with appropriate status indicators, pictures, etc.
Undo	(Nielsen, 2005)	Users find it important to be able to undo their actions.
Error Prevention	(Nielsen, 2005)	Users find it important that tools inform them how to avoid potential errors.
Control	(Nielsen, 2005)	Users find it important that they have control over the tools. Some users however, prefer automated procedures.
Learnability	(Nielsen, 1994)	Users find it important that they can easily learn how to use the tools
Satisfaction	(Weir et al., 2009), (Nielsen, 1994)	Users are not satisfied with the tools which create inconvenience in order to ensure security
Effectiveness	(Weir et al., 2009), (Nielsen, 1994)	Users report that tools were usable and easy to use, but they had difficulty in completing certain tasks successfully.
Efficiency	(Weir et al., 2009), (Nielsen, 1994) (ISO 9241-11:1998, 1998)	Users do not want to experience time delays when using the tools.
Aesthetic and minimalistic Design	(Nielsen, 2005)	Users want tools to have minimalistic design and follow modern design standards.
Accessibility	(Seffah, 2006)	Users with disabilities want to be able to use the tools.
Consistency	(Nielsen, 2005)	Users want tools to support consistency. Users might not welcome new features easily.

Control of user's personal data and transparency	(Wästlund et al., 2011)	Users want privacy tools to offer them the control of their personal data and transparency. Otherwise they will not use the tools.
Availability of tools among various platforms	Finding of this survey	Users want to use tools among different platforms, e.g. different operating systems and on their smartphones.

Table 3. User's views about usability characteristics

4.5 Discussion and Analysis of Findings

The above section has drawn on a set of usability characteristics which derived from the literature review in chapter 2 to identify which characteristics of security and privacy tools are considered important by users. More specifically the following factors were found as important by users: *easy installation, avoid registering with personal data, changes upon installation, available information and support, locatability, understandability, feedback, visibility, undo, error prevention, control, learnability and satisfaction,*

Through the interviews, however, there were identified further issues that users consider important when using these tools, such as efficiency, design, both in terms of aesthetics as well as in terms of functionality for users with special needs (accessibility), consistency, transparency, control of personal data, minimum requirements and availability of tools among different platforms.

Some of the above factors might not be yet very common to all organisations, e.g. characteristics relevant to installation, as they follow the traditional workplace environment with computers centrally administered. However, given the new trend of teleworking and of BYOD, which many large international organisations are currently following, employees use portable devices, e.g. laptops or their own personal devices. In this case employees are responsible for securing their own devices and it was essential to address as many usability aspects as possible. Factors relevant to installation, which were identified in the ENISA Report (ENISA, 2016), were investigated for that employee who needs to install a security tool on their device. Findings show that users prefer security and privacy tools which have an easy installation process, do not require them to register with their personal data for ease of use, do

not apply significant changes to the computer after installation and show to users the minimum requirements needed for the installation.

Furthermore, factors relevant to privacy were investigated for those employees who need to install use a privacy tool in case they are working in a highly confidential position which makes the preservation of privacy a top priority (e.g. bank, law firm, hospital, nuclear factory, etc.) or because they are concerned about their privacy.

In this survey it was identified that users clearly valued specific characteristics differently depending on the scope of each tool. For instance, in Ghostery, users highlighted characteristics such as *transparency, control of personal data, avoid registration with personal data, and control*, while in Tor users focused on *efficiency, satisfaction, locatability, and understandability.* It was also found that relevant literature contains many overlapping or similar characteristics using different terms such as *visibility* and *feedback.*

As is shown in the analysis, it was identified that users have mixed preferences with regard to the degree of control and tool automisation. While many users preferred to be in control of the tools, some others would prefer fully automised processes. In organisations some security tools are already configured by the IT department and minimum intervention is required by normal users. For example, the antivirus is installed by the IT administrator and scans are conducted automatically on a daily basis. While this is a practice that promotes good information security practices, this survey shows that users and especially those experienced in IT want to configure the settings of the security tools they are using. Therefore, this constitutes of a good example of a trade-off between security and usability in organisations.

An interesting finding in this survey was that Malwarebytes, had automated procedures and guided the user through the process, e.g. the user had to select from the main menu which kind of scan he preferred and then he was guided through the different steps, including selection of disks, conducting the scan and deleting the identified malware. As a result, since the tool had automated procedures and guided the users through the use, the majority of users were able to complete the steps of the scenario and use the tool successful. On the other hand, the other tools which required user's intervention and special configuration, users were not able to perform the tasks successfully. Therefore, automating procedures and guiding the user closely can help him/her use security and privacy tools successfully.

Interestingly, most users generally sought more feedback. Relative research also posits that showing many prompts to users can be frustrating and inconvenient (Yee, 2004). However, this survey shows that users need more practical and visible feedback.

Another interesting finding is that usability is also related to the availability of tools among various platforms. Recently with the advent of mobile devices, users need to be able to

use security and privacy tools on their smartphones. Employees use multiple portable devices, including laptops and smartphones, whose operating system might sometimes differ and they need to have access to the security and privacy tools from their devices.

Design plays an important role in terms of usability. In this survey, it is shown that aesthetics have an impact on users' views regarding usability. They want security and privacy tools to follow modern design trends, while they also want to be able to see what is happening in terms of security and privacy through status indicators and pictures. Another aspect which is also important but has not gained the attention of current literature in security studies is design of security and privacy tools convenient for people with disabilities.

During the interviews users also commented on the trade-off between security and usability, citing a slower browsing experience and high security leading to inability to view website content, an issue that is also under heavy discussion in relative literature (Whitten & Tygar, 1999; Weir et al., 2009). In fact, in many organisations, practices employed are not usable. For example to connect to your company's network remotely you will need to enter an one-time passcode which is generated through a secure application on your smartphone and it is valid for a limited time only. This makes the whole process not usable since the user might have to try several times to enter the appropriate passcode which might result in blocking the user from the system. Another example of not usable security in organisations is passwords that have to be changed regularly, or strict lock out policies, e.g. users are blocked from their accounts after 5 unsuccessful attempts.

This survey also shows that many users, despite being ICT students, with advanced English language and IT skills, did face usability problems in understanding some options and completing typical tasks. One therefore expects that typical users with lower technical skills, might face more difficulties when using such tools. Finally, it was evident that users needed detailed manuals. In the case of open source tools, such as Tor this is a challenge.

4.6 Conclusions

This survey has assessed a broad spectrum of usability characteristics of security and privacy tools identified in literature through the users' perspective. Though interviews and analysing the content of questionnaires, and reports it was possible to identify users' views and expectations regarding the usability of security and privacy tools.

Findings of this survey illustrate that some users had difficulty in using the English version of the tool, needed more time to adjust to English terms and would prefer the version supporting their native language. Interestingly, even experienced users, like the participants of

this survey have difficulty in understanding specific terms. Furthermore, users become confused due to the lack of consistency in terms used. They also want all security settings to be gathered together to avoid spending time looking for them and status indicators to show the tool's internal operations in terms of security and privacy. Users prefer tools that guide them closely and are intuitive, as they can complete the tasks successfully.

It is also important that security and privacy tools support the needs of people with disabilities. When users are accustomed to using one tool for a long period and the tool is updated with new features and layout, then users will form a negative attitude towards the changes, and experience usability problems. It was found that users want security and privacy tools to be available among various platforms, especially on their smartphones and among different operating systems. Furthermore, users prefer speedy help though in some cases look for detailed help.

Also, this survey has identified another complex usability issue, as many users prefer automation of some security and privacy processes, where others want control over the tool. In organisations, security settings are preconfigured by IT administrators, therefore there is limited control of users. However, this is a useful insight for BYOD users, who are responsible for configuring the security settings of the computer they are using. Another interesting finding is that users valued usability characteristics relevant to installation. More specifically, they regarded as important that the installation process is easy, that they do not have to register with personal data for ease of use, that the minimum requirements of the tool are clearly stated and that there are minimum changes on their computer after the installation of the tool. This point is interesting for people who are teleworking and for BYOD users since they can install security tools. Findings show that users are concerned about their personal data and how they are processed by tools, indicating that if users cannot control their data, or if the tool does not support transparency, trust towards the tool is low.

This survey was performed for certain tools and respondents cannot be considered as representative users. However, it was possible to elicit their opinions and suggestions and make an in-depth analysis of what users consider important regarding the usability of these tools, and for what reason and also to identify their expectations.

Chapter 5: Framework for the analysis: Factors shaping security behaviour

5.1 Introduction

Bearing in mind the aim of this Thesis was to facilitate information security management and bring the wealth of available information to the attention of security managers in a meaningful and constructive way, a Technological-Organisational-Individual framework was created. This framework divides security behaviour into three different aspects-individual, organisational and technological, each of which has an important role to play in determining security behaviour. This was done by taking the next logical step of turning the collection of findings from both the literature review and the survey on the usability factors regarding technological tools in IS into a format that would not only be clear and more easily comprehensible to security managers, but would also provide them with a kind of checklist of factors to consider that can be easily incorporated into the processes of designing and implementing ISPs.

By presenting information in the format of a framework, this Thesis offers security managers a more accessible, usable way in which to check that they are addressing a broad spectrum of aspects when it comes to designing and implementing effective ISPs. Additionally, the framework is supplemented with short, easy-to-read explanations that give security managers the essential information needed to understand every factor mentioned in the framework. Thus, security managers can have easy access at a glance to all the most significant aspects of security behaviour, which will raise their awareness of these important aspects and in turn ensure better ISPs and increased compliance.

5.2 Technological-Organisational-Individual Framework

The framework below (Figure 10) provides a comprehensive overview of the most significant factors involved in information security behaviour, classified according to three categories, namely Individual, Organisational and Technological. This allows scholars to see at a glance the many different factors at play, while also providing security managers with a clear roadmap to guide them through the complexities of security behaviour.

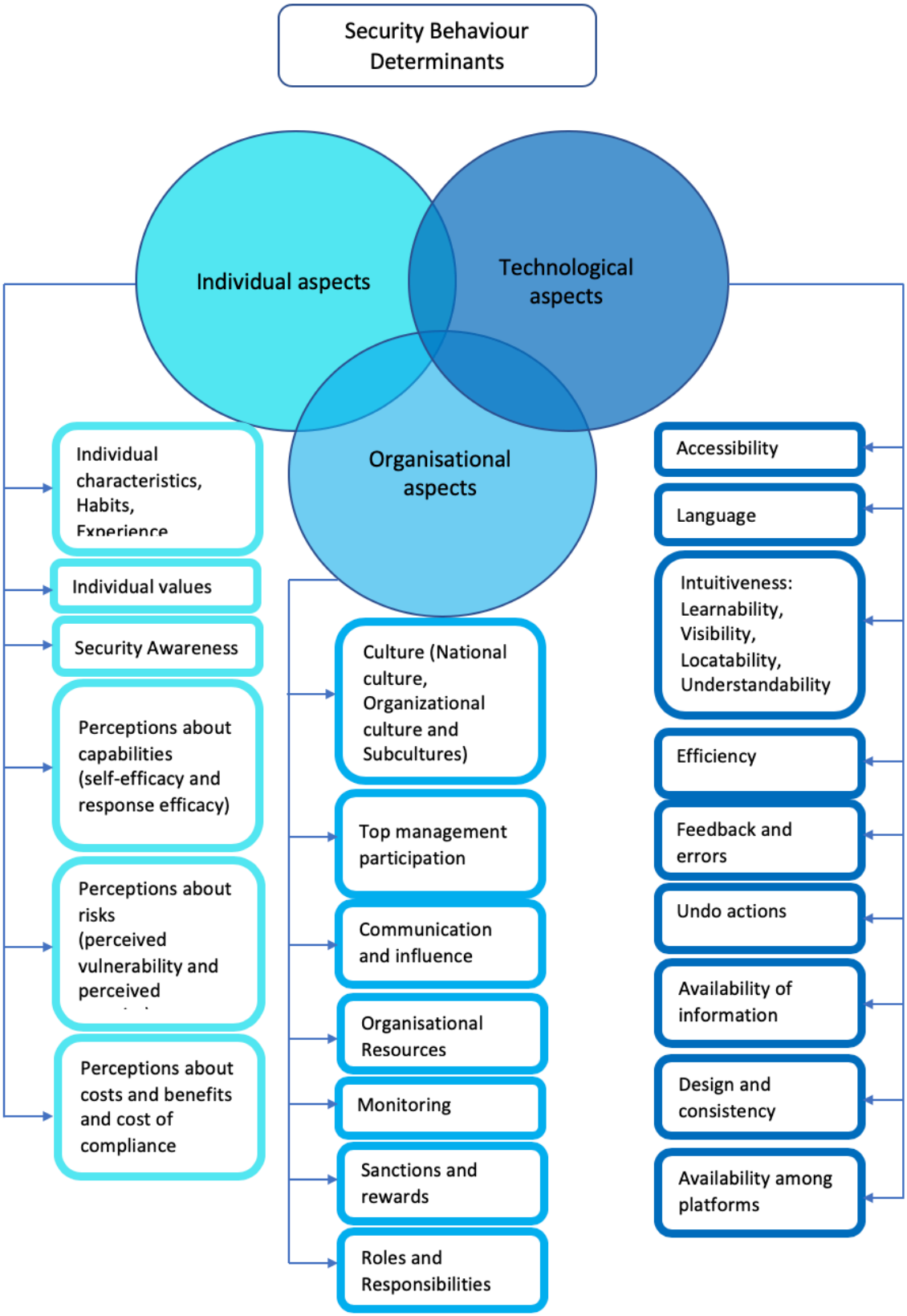

Figure 10: Technological-Organisational-Individual Framework Framework shaping security behaviour

5.2.1 Individual aspects

One significant group of individual aspects comprises *characteristics* such as age, gender, *habits* and *experience*. Literature findings suggest a correlation between age and compliance with ISPs, with older employees being more compliant (D'Arcy and Greene, 2014), as well as between the two genders with female employees showing higher compliance rates (Ifinedo, 2014). Additionally, there is evidence that greater compliance can be achieved through habitualising certain security behaviours (Son, 2011, Topa & Karyda, 2019). Similarly, an individual with experience of dealing with information security will naturally find it easier to comply with ISPs (Safa et al, 2016).

Concerning individual values, research points to the importance of ISPs being regarded as appropriate and legitimate (Son, 2011), as well as the importance of *individuals' values* being in tune with those of their organisation (Son, 2011). On the other hand it has been found that employees who follow their own interests and goals (Myyry et al., 2009), individuals who believe that their freedom is threatened by a new, strict ISP or tend to react when their freedom is restricted in this way will not comply with ISPs (Lowry and Moody, 2014).

As findings from current literature indicate, there are several types of individual *awareness* that impact on security behaviour and which therefore need to be addressed by security managers. In addition to ISP awareness (Bulgurcu et al., 2010), these include technology awareness (Dinev & Hu, 2009), general knowledge of information security (Bulgurcu et al., 2010), awareness of monitoring mechanisms and awareness of SETA programmes (D'Arcy et al., 2009).

Finally, there are a number of aspects related to *individual perceptions*. These may concern the individual's feeling of confidence in their own ability to deal with security tasks, often referred to in literature by the term of *self-efficacy*. There is reference to the individuals' perceptions about the effectiveness of their actions if they comply with the ISPs and also about the effectiveness of the ISPs; in this case this factor is identified as *response efficacy* (Ifinedo, 2012; Herath & Rao, 2009a). There are also individual *perceptions regarding security risks* to their organisation and their severity (Siponen et al., 2014). There are perceptions of how individuals perceive the possible *benefit* of compliance including rewards, positive feelings such as contentment and the *cost of non-compliance* including sanctions and negative feelings such as shame, embarrassment, etc. (Bulgurcu et al. (2010). There is also the *cost of compliance* with ISPs, mainly in terms of time, effort and convenience (Bulgurcu et al. (2010).

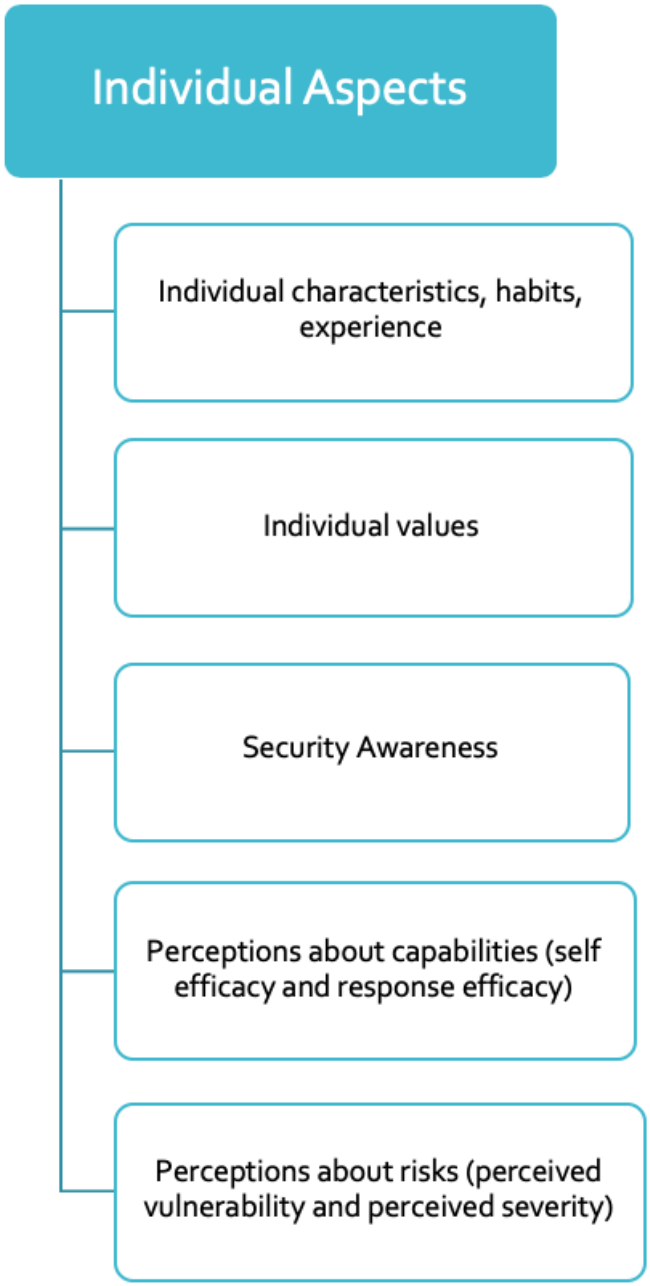

Figure 11: Factors shaping security behaviour: Individual aspects

5.2.2 Organisational aspects

According to literature, one significant aspect of security behaviour is *culture*, which can include national culture, organisational culture and subcultures (Kolkowska, 2011). In terms of organisational culture, flat management encourages employees to give feedback about security issues and comply with ISPs (Connolly et al., 2015). When employees' feedback is taken into account during the ISP creation process, this leads to ISPs that are not cumbersome or overlooked (Kirlappos et al., 2015).

Top management participation is also found to influence employees' security behaviour (Hu et al., 2012). More importantly, top managements' actions need to be visible to employees to convey the message that ISP compliance is important and that since top management is complying with ISPs all other employees are expected to follow their example (Hu et al., 2012).

Communication among employees within an organisation is regarded as a factor that motivates them to comply with ISPs (Ifinedo, 2014). For example, through formal or informal meetings employees exchange views about security issues. One significant aspect of communication is knowledge sharing (Safa et al., 2016), where employees pass their security knowledge on to colleagues. An important role is also played by *social influence*, namely the way in which employees' security behaviour is influenced by others' actions and beliefs (Herath & Rao, 2009a).

Organisational resources including help from experts, time to get used to new ISPS, training and seminars can all motivate users to comply with ISPs (Pahnila et al., 2007) Furthermore, the quality of the ISPs with regard to easily understandable *language* and up-to-date content is also significant in determining security behaviour (Pahnila et al., 2007).

According to literature, a further important organisational aspect is the existence and visibility of *monitoring controls*, which has been found to influence employees' security behaviour (Herath & Rao, 2009b).

Likewise, *sanctions and rewards* are security behaviour determinants (Bulgurcu et al., 2010), though it is important to note that sanctions and rewards show contradictory findings. This can be due to the fact that There are cases where sanctions and rewards have no impact on employee security behaviour (Siponen et al., 2014; Pahnila et al., 2007; Son, 2011).

Figure 12: Factors shaping security behaviour: Organisational aspects

5.2.3 Technological aspects

There are a number of important technological aspects which are relevant to the usability of security tools, which according to literature may impact on security behaviour and consequently on ISP compliance (Topa & Karyda, 2018). It is therefore essential that security managers be made aware of these security behaviour determinants and take the appropriate steps to ensure that any security tools used by the organisation have optimum usability.

One significant aspect is that of *accessibility* (Topa & Karyda, 2018), which relates to security tools being accessible to people with disabilities.

Language comprises another important aspect of security tools. Literature findings suggest that the language used has to be clear and plain, easy to understand, and without too many technical terms. This is particularly important for non-IT employees (Topa & Karyda, 2018).

A significant technological aspect of security tools that covers a broad range of closely-related features is *intuitiveness*. As in the case of language, the emphasis is on how easy the tools are to use, but more specifically how a number of features of the tool can work together to make the whole process of using them, even for the first time, seem intuitive. Thus, one feature is learnability, namely that tools need to be easy for users to learn how to use (Topa & Karyda, 2018). Tools also need to have security settings that are easily locatable (locatability) and visible (visibility) (Topa & Karyda, 2018; Furnell, 2010, Johnston et al., 2003). For example, users need to be able to find the security settings easily without spending too much time and also there should be security indicators (namely graphs, pictures or illustrations) to show them what is happening inside the system in terms of security. Additionally, they should naturally guide the users, helping them understand how to use them (understandability) (Topa & Karyda, 2018; Whitten & Tygar, 1999).

To maximise their usability and in turn achieve better ISP compliance, security tools should be *efficient* and not create additional time delays or inconvenience to users (Topa & Karyda, 2018; Whitten & Tygar, 1999).

A further usability characteristic that can improve security tools' effectiveness is the provision of *feedback* to users (Murayama et al., 2012). Users need to be able to receive information regarding *errors* and *error prevention* as well as being able to *undo their actions* (Topa & Karyda, 2018).

Availability of information is regarded as a usability characteristic (Topa & Karyda, 2018). This means that users should have easy access to manuals and other help and support

when needed. This may be particularly useful when a security tool is new or just being introduced.

Two more aspects of usability that may affect users' security behaviour are *design* and *consistency*. Literature suggests that users prefer tools with a minimalist design, while users also show a preference for tools that do not undergo radical changes when they are updated (Topa & Karyda, 2018).

Availability among various platforms is another aspect of usability. Users need to have security tools on their computers and portable devices, including laptops, tablets and smartphones (Topa & Karyda, 2018).

Furthermore, among the main usability factors, this PhD Thesis has investigated some more characteristics for cases where employees telework and therefore use the company's laptop or use their own devices, following the practice "Bring your own device". In this case they will be responsible for downloading and installing the appropriate security tools. For this reason factors relevant to installation should be considered. These factors include easy installation, minimum requirements for installation e.g. specific operating system should be clearly stated, minimum changes upon installation should take place and users should not have to register with their personal data to use the tool.

Other factors to be considered in this framework as part of the technological factors are factors relevant to privacy. In cases where employees need to use privacy tools, e.g. if they are working in a highly confidential position where they need to preserve their privacy and anonymity, e.g. in a top law firm where lawyers need to exchange emails with the clients without relevelling their location or personal information. In this case users are concerned about the *control over* their *personal data* and how their personal data are processed. *Transparency* during the processing of users' data is a usability factor that motives users to use privacy tools.

Another usability characteristic is *control*. This factor shows mixed findings. In some cases users want to have the control of security and privacy tools and select the options they want to achieve optimum security. However, there are also cases where employees prefer automated tools so that they do not have to select and configure security settings themselves.

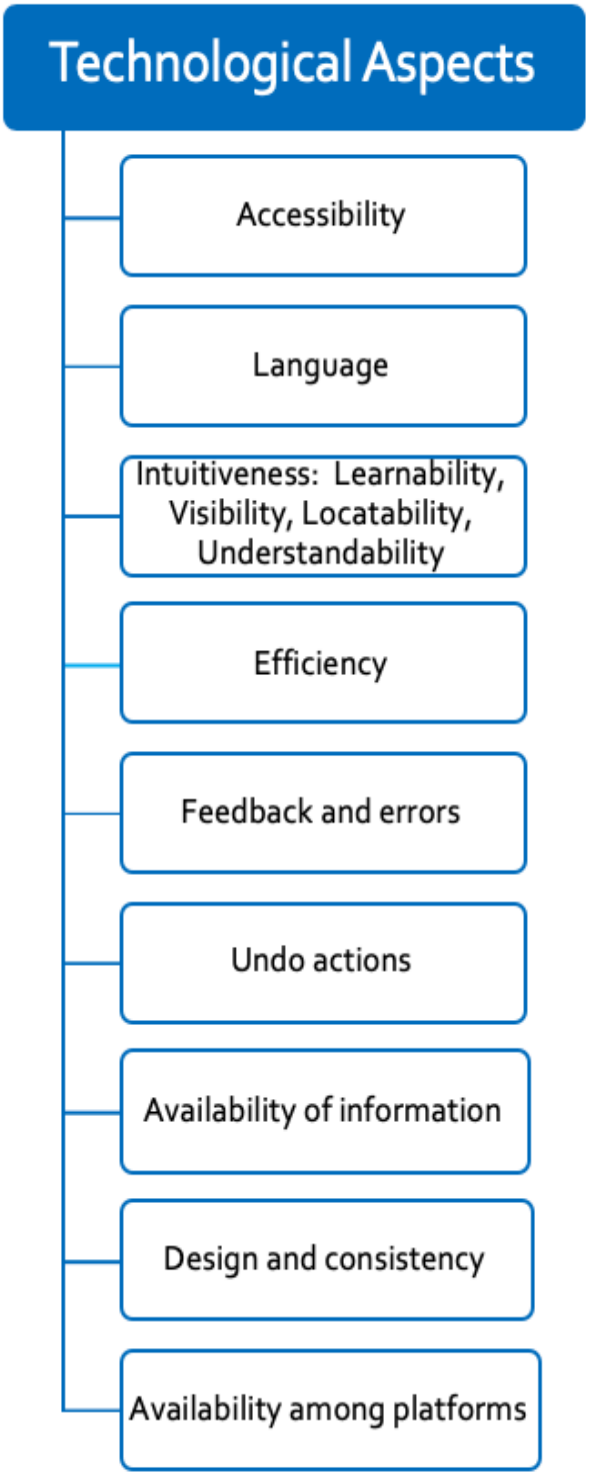

Figure 13: Factors shaping security behaviour: Technological aspects

5.3 Conclusions

The above section analyses the Technological-Organisational-Individual framework that was created based on the literature review and analysis of ISP compliance and security behaviour and on the usability survey that is later used for the analysis of security management practices. This framework can also facilitate security managers gain a comprehensive understanding of all the factors influencing security behaviour. These factors are grouped under three main categories, including individual, organisational and technological aspects. It is important to mention that these factors are considered from the user's perspective. As a result, by looking at the framework security managers can have a clear idea of the factors that motivate users to comply with ISPs and use security and privacy tools. This framework can act as checklist for security managers when implementing their security managers, as it provides a comprehensive approach of all the aspects they need to consider to address the "human aspect" during the implementation of security policies and practices.

In the following chapters of this PhD Thesis, the Technological-Organisational-Individual framework will guide the analysis of current security management practices that are described the ISO 27001, 27002, 27003 and 27005 Standards and followed in in a real life organisation. Finally, based on the factors that are described in this framework a set of practical guidelines are provided to security managers on how to exploit relative knowledge and design their security management practices accordingly.

Chapter 6: Analysing security management Standards: ISO 27001, 27002, 27003 and 27005

6.1 Introduction

The extensive review of current literature conducted to determine all the factors that affect security behaviour and the subsequent Technological-Organisational-Individual framework devised to organise those factors into clear and more manageable groups generated a wealth of useful information that is relevant to and can enhance information security practices. The next step was to explore the practices, which are currently recommended to determine the amount and quality of information that is currently available to security managers. To achieve this, the present Thesis focused on the most widely used set of security guidelines applied by organisations, namely the ISO Standards and in particular ISO 27001, 27002, 27003 and 27005. By analysing these ISO standards, the objective was first to identify what practices are currently recommended to security managers and then to compare them against the findings of the literature review and the framework. This would make it possible to reveal any gaps or discrepancies that exist between the aspects covered by the framework and the guidelines currently available to security managers through the ISO standards. Thus, this gap analysis could then lead to the devising of essential guidelines for security managers that they currently do not have access to as well as complementary recommendations to improve their security practices. The following section therefore looks at the provisions laid down in ISO standards 27001, 27002, 27003 and 27005 identifying any gaps or shortcomings and highlighting crucial areas where security managers can benefit from the far more detailed findings of related research and the framework based on these which this Thesis offers.

The following analysis of ISO 27001, 27002, 27003 and 27005 and the subsequent gap analysis were conducted using the factors identified in the review of current literature and employed in the framework, which resulted from the findings of that review.

6.2 Standards guiding information security management

Information security management is the process of applying security practices and controls to safeguard the organisation's information assets. Aiming to preserve the confidentiality, integrity and availability of information, security managers apply security practices and controls from a variety of security frameworks including COBIT, the Standards

of the National Institute of Standards and Technology (NIST) and the ISO/IEC 27000 family of security standards.

COBIT version 5 is a framework for IT management and governance, which encompasses general IT practices and business objectives (IT Governance Institute, 2008) and deals with IT risk mitigation and IT risk management (COBIT, 2007; Susanto et al., 2011). Designed to be compatible with other standards COBIT provides guidance for security management requirements similar to ISO 27001 and ISO 27002 (Lambrinoudakis, 2013; Susanto et al., 2011; Năstase et al., 2009).

The NIST 800-30 framework provides security managers with insights into risk management, describing the steps they should follow to identify risks, apply controls and enhance security, similar to ISO 27005 (Stoneburner et al., 2002; Lambrinoudakis, 2013).

ISO information security standards guide security managers on how to design and implement practices towards establishing an ISMS and propose security controls. ISO standards have many advantages including common terminology, providing a basis and an understanding of security requirements and making sure that the security controls are in accordance with rules and standards that are accepted on an international level (Tsohou et al., 2010). Recently, the number of ISO 27001 certifications being issued worldwide has increased steadily, rising 20 per cent for ISO 27001 certificates from 2016 to 2017 (ISO Survey, 2017). Given their widespread use, this Thesis focuses on ISO 27000 standards and in particular on ISO 27001, 27002, 27003 and 27005.

Requirements described in ISO 27001 include the responsibilities of top management, the creation of ISPs, the identification of risks, the implementation of the appropriate controls and security countermeasures. It also prescribes the provision of organisational support, such as the availability of resources, determining and enhancing employees' competence and awareness, and promoting communication. Finally, it describes monitoring and auditing.

ISO/IEC 27002 contains directions on security controls for safeguarding the organisational assets (ISO 27002, 2013). Following ISO 27002, security controls need to satisfy regulatory, legal and contractual requirements, address different aspects of the socio-cultural environment and ensure organisations' business objectives. In ISO 27002 there are 35 main security categories and 114 security controls which include mostly technical measures such as cryptography or communication security; however, it offers guidelines on 'human resource security' including security training (ISO 27002, 2013). Security training informs employees on their accountability and on the consequences for themselves or their organisation in case of security violations. It also specifies sanctions for ISP violations, rewards for

outstanding achievement in information security and defines monitoring and incident reporting mechanisms and processes.

ISO/IEC 27003 describes the processes and steps needed to create and establish an ISMS, from inception to implementation (ISO 27003, 2010). It advises on gaining senior management approval, defining the ISMS scope, identifying the information security requirements, carrying out risk assessment and risk treatment and designing and implementing the ISMS. Further, it offers guidance on designing ISPs and creating SETA programs, describing the different responsibilities of stakeholders and giving instructions about monitoring.

ISO/IEC 27005 focuses on the risk management process (ISO 27005, 2011). It does not specify which risk management approach to follow; it only stipulates the requirements needed to support an ISMS with reference to the constraints security controls need to address such as ease of use and culture.

6.3 Gap analysis

In this section all the factors that are included in the framework, namely individual, organisational and technological, are used to analyse the information security practices provisioned in ISO 27001, 27002, 27003 and 27005 Standards.

6.3.1 Organisational aspects

6.3.1.1 Culture

ISO 27003 (section 6.3) indicates that security managers need to consider the socio-cultural environment when defining the ISMS scope, and especially when defining the ICT scope and boundaries (ISO 27003, 2010). While this is an important general consideration, scholar research goes further, identifying the role of *national cultures* (Dinev et al., 2009), *organisational culture* (Hu at el., 2012) and *subcultures* in shaping employee security behaviour (Kolkowska, 2011).

6.3.1.2 Organisational Resources and Training Programs

ISO 27001:2013 (section 7.1) stipulates that organisations need to provide the appropriate resources for the establishment, implementation, maintenance and improvement of the ISMS but lacks specific guidance on the nature of these resources. Literature provides further insights on the different resources that facilitate individuals and motivate them to comply with ISPs. These resources include training, communication practices (such as posters, newsletters and notices), easily accessible ISPs, help from experts and adequate time to become familiar with ISPs (Pahnila et al., 2007; Herath & Rao, 2009a).

ISO 27002:2013 (section 7.2.2) and literature agree on the importance of implementing SETA programs. Related literature has more insights to offer, highlighting that individuals' perceptions about the effectiveness of their ISP compliant behaviour can make a difference (Herath & Rao, 2009a). Furthermore, consequences to employees, i.e. rewards and sanctions (Bulgurcu et al., 2010) are not mentioned.

Although ISO 27003:2010 (section 9.4.2) recommends that SETA programs inform employees about security risks and threats in general, related research suggests that employees can benefit from awareness of threats and vulnerabilities that are specific to their organisation (Ifinedo, 2012; Siponen et al., 2014) and their severity (Siponen et al., 2014, Herath & Rao, 2009a; Vance et al., 2012; Pahnila et al., 2013). This information derives from risk assessments conducted in organisations as mentioned in ISO 27001:2013 (section 6.1.3) and ISO 27003:2010 (section 8.2) but is currently communicated only to security personnel and top management and not to all the employees.

However, apart from the provision of tangible resources, literature suggests that there are other non-tangible organisational aspects that influence employees to comply with ISPs, such as job satisfaction. Literature shows that for employees who do not work in IT positions or in IT-related companies (D'Arcy & Greene, 2014) if they are satisfied with their job they will comply with ISPs. Another factor that motivates employees to comply with ISPs is when their contribution is valued (Shropshire et al., 2015). These more subtle, non-tangible aspects, which are not addressed in the ISO Standards, can be viewed as organisational in so far as the organisation is responsible for promoting the conditions, environment or attitudes conducive to these employee perceptions.

6.3.1.3 Top management's involvement and compliance

In ISO 27001 while it is proposed that top management should act in a way that promotes leadership and commitment towards an ISMS, it is not specified how security managers are to achieve this (ISO 27001, section 5.1, 2013). ISO 27002 (section 5.1.1) suggests that upper management should approve ISPs, but in real terms this could be limited to top managers simply adding their signature or official stamp to a document. The guidelines make no reference to top management's visible involvement in or commitment to ISP compliance. However, literature goes much further in advocating the active role top management can play in influencing security behaviour (Hu et al., 2012). There is no clear guidance of what top management can do in practice to foster leadership and to show commitment towards ISPs.

6.3.1.4 ISP content

ISO 27003 (section 9.2.3) and ISO 27001 (section 5.2) provide guidelines on designing ISPs, specifying that ISPs need to be sufficiently summarised, easily accessible and appropriate for the purpose of the organisation (ISO 27001, 2013; ISO 27003, 2010). While these basic guidelines are useful, they do not cover many other important aspects of design and implementation such as the type of language used in ISPs, aspects concerning their availability and form or how they are communicated to employees (Pahnila et al., 2007).

6.3.1.5 Assigning Roles and Responsibilities

ISO 27001:2013 (section 5.3), ISO 27002:2013 (section 6.1.1) and Annex B in ISO 27003:2010 provide general guidance with regard to the roles and responsibilities employees should be assigned in terms of Information Security when carrying out information security tasks. For example, the Chief Information Security Officer has general responsibility and authority over information security while employees are expected to take responsibility for information security in their working environment. This could be interpreted as a rather grey area. Thus, although the responsibilities for each role are listed, there is potential for lack of clarity regarding each user's own responsibilities, which may lead to conflicting perceptions over the exact boundaries between respective responsibilities (Kolkowska, 2011).

6.3.1.6 Sanctions and rewards

Regarding sanctions, ISO 27002:2013 (section 7.2.3) specifies establishing a disciplinary process for security policy violations. However, as research reports mixed findings on the effectiveness of sanctions for non-compliance (Sommestad et al. 2014; Son, 2011; Herath & Rao, 2009a; Herath & Rao, 2009b). This information is not included in the ISO Standards giving security managers the impression that sanctions for non-compliance will be effective.

Concerning rewards for compliance, ISO 27002:2013 (section 7.2.3) recommends rewarding employees for outstanding achievement in terms of information security. This practice is supported by literature. For example, Bulgurcu et al. (2010) found that individuals who believe that ISP compliance will lead to tangible and intangible rewards (e.g. pay raise, personal mention and appreciation in oral or in written reports, promotions and reputation) are more motivated to adhere to security policies. It is clearly not within the remit of ISO Standards to make highly specific recommendations to organisations regarding the form in which they might implement rewards. However, this is an area where security managers would certainly benefit from having practical suggestions. Moreover, there is also the issue of employee awareness of any potential rewards, since if employees are unaware of the existence of possible rewards for good security behaviour those rewards cannot act as an incentive.

6.3.1.7 Monitoring controls

ISO 27001:2013 (section 9.1) and ISO 27002:2013 (section 12.4) stipulate that monitoring plays a key role in security management, but do not go into detail concerning the most effective aspects of monitoring such as the existence and visibility of monitoring and detection mechanisms. Moreover, there is no reference to the practical difficulties involved in monitoring all different aspects of security behaviour (e.g. checking whether employees are noting down passwords) and the consequent value of adopting a combination of different forms of monitoring controls.

6.3.1.8 Communication and influence

Social influence is not addressed in ISO 27000 Standards. According to literature, employees who believe that significant others, such as their superiors and colleagues, expect them to comply with ISPs or see them following ISPs, are more inclined to comply (Siponen

et al., 2006; Pahnila et al., 2007; Herath & Rao, 2009a; Ifinedo, 2012; Siponen et al., 2014; Bulgurcu et al., 2010; Herath & Rao, 2009b; Ifinedo, 2014; Hu et al., 2012).

Both ISO 27001:2013 (section 7.4) and literature recognise the need for communication, though literature offers more extensive insights, referring to the benefits of knowledge sharing (Ifinedo, 2014). Furthermore, according to Dinev & Hu (2007), individuals with an IT background exchange views about security issues and tools, while basic IT users do not. Literature refers to the relationships that are formed within colleagues who share the same security views (Safa et al., 2016).

Another aspect of communication is incident reporting which is identified by both ISO 27002:2013 (section 16.1.1) and literature (Safa et al., 2016).

6.3.2 Individual aspects

6.3.2.1 Accommodating individual characteristics, experience, values and habits

In spite of the abundance of literature on various individual characteristics and their influence on security behaviour, the ISO 27000 series make very little reference to individual characteristics. Employees' experience is mentioned in ISO 27001 (section 7.2) (ISO 27001, 2013), though this is not elaborated on in any detail. Current literature identifies a wide range of security behaviour determinants such as age (Pahnila et al. (2013), gender (Herath & Rao, 2009b), habits (Vance et al., 2012) and values (e.g. perceived value congruence Son (2011), openness to change (Lowry and Moody, 2014) r and reactance proneness (Lowry and Moody, 2014)).

6.3.2.2 Perceptions regarding capabilities

Employees' competence is mentioned in ISO Standards (ISO 27001:2013 (section 7.2)) but there is no reference to employees' confidence in complying with ISPs (Siponen et al., 2006; Herath & Rao, 2009a; Vance et al., 2012; Ifinedo, 2012; Siponen et al., 2014).

6.3.2.3 Cost of compliance

The ISO 27001, 27002, 27003 or ISO 27005 standards do not refer to cost of compliance, namely the additional burden on employees in terms of time or effort. According

to literature, employees who consider security policies as an impediment to their work or as time-consuming are less likely to follow them (Bulgurcu et al., 2010).

6.3.2.4 Security Awareness

ISO 27001:2013 (section 7.3) provides guidelines on increasing employees' awareness of ISPs, of how they can contribute to organisational security and on the negative outcomes from non-compliance with ISPs and failing to apply security controls. However, literature suggests that there are more types of awareness that play a part in ISP compliance, including technology awareness (Dinev & Hu, 2007), general knowledge about information security (Bulgurcu et al., 2010), awareness of the limitations of security tools, awareness of monitoring mechanisms and awareness of SETA programs (D'Arcy et al., 2009).

6.3.2.5 Perceptions regarding risks

There is no reference in ISO standards about the perceptions of employees regarding threats and vulnerabilities in their organisation. According to literature employees' perceptions about threats and vulnerabilities specific to their organisation (Ifinedo, 2012; Siponen et al., 2014) and their severity (Siponen et al., 2014, Herath & Rao, 2009a; Vance et al., 2012; Pahnila et al., 2013) can motivate them to comply with ISPs.

6.3.3 Technological aspects

6.3.3.1 Selecting appropriate security controls

Regarding the use of security controls, there is a substantial amount of information in the ISO 27000 series. ISO 27001:2013 in Annex A provides an extensive list of security controls and control objectives which are further described in ISO 27002:2013, while ISO 27003:2010 (section 8.3) provides guidance on the selection of the control objectives and controls (ISO 27003, 2010). ISO 27005:2011 (section 9.2 and Annex F) offers guidelines that concern the use of technological controls, including ease of use, compatibility and performance issues, and financial constraints, etc.

While there is reference to the fact that security controls should be easy to use, this is a broad term and it does not inform security managers of all the usability subfactors that are involved in making a security tool easy to use. These subfactors are accessibility (security tools are available to users with disabilities), language (security tools have language that easy to

understand, e.g. without including many technical terms) and intuitiveness (security tools' settings are easy to find, security tools include indicators showing users what is happening in terms of security, security tools are easy to learn and easy to understand how to be used) (Topa & Karyda, 2018). Automation is another usability characteristic that make tools intuitive, as it is easier for users to users tools correctly if processes are automated and there is limited control over the tool (Topa & Karyda, 2018). Other factors are feedback and errors (security tools provide feedback messages to users and messages about errors), error prevention (security tools prevent users from making errors), undo of actions (security tools allow users to undo their actions), efficiency (security tools are efficient in use without time delays) and availability of tools among various platforms (security tools are available among different operating systems and platforms) (Topa & Karyda, 2018). Other usability characteristics include minimalistic design (security tools show only the relevant information and follow modern trends), consistency (security tools follow a consistent form e.g. after updates) availability of information and support (security tools have available help and support) and control and automation (security tools offer users the opportunity to configure the security settings themselves or they give limited control and the processes are automated) (Topa & Karyda, 2018). For users who use organisational portable devices or their own personal devices for teleworking purposes, usability characteristics relevant to installation that need to be considered (Topa & Karyda, 2018). Privacy characteristics such as transparency and control of users' data are also part of the usability characteristics to be considered for users' who are concerned about their privacy (Topa & Karyda, 2018).

Security management practices	**Reference in ISO Standards**	**Factors not adequately addressed**
Consider the socio-cultural environment when defining the ISMS scope	ISO 27003:2010 (section 6.3)	• *National cultures* (Dinev et al., 2009), • *Organisational culture* (Hu at el., 2012) *Subcultures* (Kolkowska, 2011)
Provision of resources for the establishment, implementation,	ISO 27001:2013 (section 7.1)	• *Resources* including training, communication practices (such as posters, newsletters and

maintenance and improvement of the ISMS		notices), easily accessible ISPs, help from experts and adequate time to become familiar with ISPs (Pahnila et al., 2007; Herath & Rao, 2009a).
Implementation of SETA programs (ISO 27002:2013, section 7.2.2)	ISO 27002:2013 (section 7.2.2)	• *Individuals' perceptions about the effectiveness of their ISP compliant behaviour* (Herath & Rao, 2009a) • *Individuals' perceptions about rewards and sanctions* (Bulgurcu et al., 2010)
Inform employees about security risks and threats in general through SETA programs	ISO 27003:2010 (section 9.4.2)	• *Individuals' perceptions about threats and vulnerabilities relevant to their organisation* • *Job satisfaction* especially for non-IT employees or employees in non-IT companies (D'Arcy & Greene, 2014). • Employees' *contribution is valued* (Shropshire et al., 2015).
Top management should act in a way that promotes leadership and commitment towards an ISMS	ISO 27001:2013 (section 5.1)	• *Top management's visible involvement* in or commitment to ISP compliance (Hu et al., 2012)
Guidelines on designing ISPs	ISO 27003:2010 (section 9.2.3), ISO 27001:2013 (section 5.2)	• *Type of language*, • *Availability of ISPs* • *Communication of ISPs*

Guidelines on assigning Roles and Responsibilities	ISO 27001:2013 (section 5.3), ISO 27002:2013 (section 6.1.1) and Annex B in ISO 27003:2010	• *Conflicting perceptions over the exact boundaries between respective responsibilities*
Establishing a disciplinary process for security policy violations	ISO 27002:2013 (section 7.2.3)	• *Individuals' perceptions about punishment*
Rewarding employees for outstanding achievement in terms of information security	ISO 27002:2013 (section 7.2.3)	• *Individuals' perceptions about rewards (both tangible and intangible)*
Monitoring	ISO 27001:2013 (section 9.1) and ISO 27002:2013 (section 12.4)	• *Visibility of monitoring and detection mechanisms.*
Communication	ISO 27001:2013 (section 7.4)	• *Social influence* (*significant other's expectations and behaviour)* • *Knowledge sharing*
Experience	ISO 27001:2013(section 7.2)	• *Individual characteristics (age and gender)* • *Individual values* • *Habits*
Employees' competence	ISO 27001:2013 (section 7.2)	• Employees' *confidence* in complying with ISPs
Employees' awareness of ISPs	ISO 27001:2013 (section 7.3)	• *Technology awareness* (Dinev & Hu, 2007) • *General knowledge about information security* (Bulgurcu et al., 2010) • *Awareness of the limitations of security tools* • *Awareness of monitoring mechanisms* and *awareness of*

		SETA programs (D'Arcy et al., 2009).
List of security controls and control objectives. Guidelines for using technological controls with ease of use.	ISO 27001:2013 in Annex A, ISO 27003:2010 (section 8.3) and ISO 27005:2011 (section 9.2 and Annex F)	• *Accessibility* • *Intuitiveness* • *Language* • *Feedback and errors* • *Error prevention* • *Undo of actions* • *Efficiency* • *Availability of tools among platforms* • *Availability of information and support* • *Control* and automation • Characteristics relevant to installation • Characteristics relevant to privacy

Table 4: Gaps in security management practices based on ISO 27001, 27002, 27003 and 27005

6.4 Conclusions

A thorough analysis of ISO Standards 27001, 27002, 27003 and 27005 indicates that, while there is an overlap between the information covered in these standards and current literature, there are also significant gaps. The result in terms of information security management is that security managers currently follow the guidelines stipulated by ISO without a complete understanding of security behaviour, which in turn may lead to inadequate practices, resources or tools.

Significant areas in which security management practices are not adequately addressed or not covered due to the nature of the ISO Standards include: cultural aspects; certain aspects of top management's involvement; job satisfaction; employees' contribution is valued;

different types of awareness, the effectiveness and awareness of sanctions and rewards; individual values, perceptions and characteristics (age and gender); habits; individual's perceptions about risks; individual's perceptions about their confidence in following ISPs; and more detailed guidance on the usability characteristics of security tools. By conducting the gap analysis in the light of current research findings, this Thesis adds important information to the large body of existing literature on security behaviour, while also identifying numerous ways in which security management practices could be enhanced to offer security managers valuable help that is not currently available to them.

Chapter 7: Case Study: Analysing Security Management Practices

7.1 Introduction

Current literature on information security behaviour provides a wealth of theoretical information that can be considered useful to security managers, while an analysis of the ISO Standards 27001, 27002, 27003 and 27005 also offers general guidelines on the ways in which security managers can deal with security behaviour and ISPs. The research objective of the case study described in the following section is to analyse how information security is dealt with in reality, drawing on the framework of factors as the basis for the analysis.

Through the case study it was also able to validate the applicability of the framework addressing individual, organisational and technological aspects which has been described in Chapter 5, with the aim of facilitating information security management. This case study sheds light on how findings from scholar research can be applied in practice on a day-to-day basis, and to identify aspects of the framework that were implemented.

Overall, this case study involves an organisation which constitutes an example of good information security practices achieved through implemented information security management practices that focus on organisational aspects, on the individual and on technology. In the interests of security, privacy and confidentiality, the organisation remains anonymous.

7.2 Research Outline

Research was carried out over a three-month period in one branch of a large organisation. The first objective was to analyse the information security management practices which were currently applied and, using the framework presented in chapter 6 as the basis for the analysis, compare them with the extant literature findings and standards' guidelines. Through the case study it was possible to identify new and effective practices followed by the organisation which have not yet been widely researched and can add to current knowledge in this field.

Subsequently, through the analysis of current practices shortcomings in terms of security management were identified, leading to the proposal of potential improvements to further enhance security management practices based on research conducted by Topa and

Karyda (Topa & Karyda, 2019). Finally, the applicability of factors included the framework were tested.

The case study was conducted over the course of three months. Research data was gathered in three ways: discussion and interviews with employees and other personnel in the IT security department; general observation of both employees' and management's security behaviour; and analysis of documentation related to IS management practices and ISPs. Interviews were conducted with the IT security personnel and members of the management team in the IT security department to gain a comprehensive idea of how this organisation operates in terms of information security. Additional insights were gained through observation of employees and managers in their day-to-day security tasks as well as the organisation's environment. Further, through a detailed review of current information security policies, it was possible to formulate a clear picture of the context of the organisation and identify the information security practices currently followed. During this case study the process of creating and developing new ISPs was observed.

7.3 Security management practices followed

The Technological-Organisational-Individual framework presented in chapter 5 was used as the basis of the analysis in of security management practices followed in the organisation. In addition, it was possible to test the applicability of factors included in this framework in an organisation. Below there are the practices that are implemented in practice by the large organisation and address the three categories of factors that are included in the Technological-Organisational-Individual framework.

7.3.1 Practices based on Organisational factors

7.3.1.1 The role of Culture

Employees of this organisation are of different nationalities. Given that it is a multi-cultural working environment, no significant behaviour trends originating from employees' national culture were observed. Rather, there is a strong emphasis on *organisational culture* through practices that promote organisational goals and values (in particular equality, communication and collaboration).

7.3.1.2 Top management participation

Top management follows security practices, by securing their computers with passwords and creating guest accounts when access to their computer is needed by other colleagues, etc.

7.3.1.3 Organisational Resources and Content of ISPs

This organisation follows information security practices that are stated in ISO 27001 Standard, including the provision of a facilitating environment in terms of *resources* (security documents, posters, cards, training, etc.) which is a practice that motivates users to comply with ISPs (Herath & Rao, 2009a). All employees have access to information regarding information security practices. There is formal documentation for raising employees' security *awareness* and informing them of the appropriate security behaviour. On the intranet there is also an online guide to security threats and what employees should be aware of when browsing online such as phishing, spamming, opening emails etc. Additionally, employees have access to a website on the intranet which informs them about different issues of the organisation, including-IT and security issues.

In various visible locations, such as at the entrance to the building, large posters inform employees about how to deal with security issues such as phishing (Figure 14). Furthermore, on various stands located in different work areas employees can pick up cards which promote IS security. These cards use illustrated messages to highlight the difference between good and bad security practices e.g. a picture of a desk where the desktop computer and mobile devices such as smartphones and tablets are in clear view, unlocked and unattended, which is in sharp contrast to the image next to it of a desk where everything is organised, the desktop computer is locked and there are no mobile devices on the desk. The caption "Better safe than sorry" below the images clearly suggests that users should not leave their devices unattended and unlocked when out of their office. Another card, similar to this one shows the picture of a desk with multiple devices and personal items left unlocked and unattended followed by the caption "LOCK IT or LOSE IT". This is a card indicating the consequences that will take place if the employees do not follow the clear desk policy of the organisation (Figure 15). Figures 14 and 15 were created for this Thesis to simulate the posters and the cards of the large organisation.

This organisation operates in various locations and for this reason employees need to travel to different places for business purposes. Meanwhile, the organisation is shifting from the traditional workplace to a more flexible teleworking scheme, where employees have

portable devices such as laptops instead of desktops and can work from different locations or from their homes when travelling, and so on. There is thus a need for employees to be adequately informed of the security threats and risks that might take place when teleworking and form the appropriate security behaviour. The organisation has identified this need and has developed a security policy for teleworking, written in *language* that is easy for employees to understand and which does not include many technical terms.

Figure 14: Large posters informing employees about security threats

Figure 15: Cards showing the consequences of employees' non-compliance with ISPs

7.3.1.4 Communication and influence

All employees of the organisation participate in formal and informal meetings on a daily basis to discuss work issues and make decisions. This is facilitated by a general organisational culture that encourages *communication* between employees. It is common practice for colleagues to visit each other in their offices or communicate through phone calls or video teleconferencing. Communication plays a pivotal role in the day-to-day functioning of the organisation, which strongly encourages collaboration and also ensures that employees discuss work issues with superiors and co-workers. In this way, employees are encouraged to share their knowledge with colleagues on all work-related issues, including security practices. It is also customary for employees to consult more experienced colleagues, while those with greater experience in any given area readily offer advice and support. This openness and willingness to help on the part of more experienced employees ensures that those less knowledgeable about information security have access to the necessary support and do not feel intimidated by a lack of expertise in dealing with IS practices, leading to *self-efficacy*.

Furthermore, it was observed that employees ask for IT experts' help at the helpdesk on any IT or security-related issues. Resource availability, e.g. help from experts, is a factor which influences employees to comply with ISPs (Herath et al., 2009a).

7.3.1.5 Roles and Responsibilities

The organisation has clearly assigned *roles and responsibilities* in terms of information security with the IT security department of the organisation being responsible for ensuring information system security. In every department, e.g. Finance, Communication etc., there is an administrator responsible for carrying out admin operations. This person also acts as an information security officer. More specifically, he/she is the point of contact for security incidents that might take place and is responsible for reporting them to the IT security department. As stated in relevant literature, this person serves as a "security champion" by communicating the importance of ISP compliance to employees (Ifinedo, 2012).

7.3.1.6 Sanctions and Rewards

Regarding *sanctions* and *rewards*, the organisation's security management practices do not include specific sanctions for employees who fail to comply with ISPs. Bearing in mind that sanctions have mixed results in terms of effectiveness (Topa & Karyda, 2016), they might not be effective in this particular organisation and would conflict with its organisational values.

7.3.2 Practices based on Individual factors

7.3.2.1 Habits

Cards illustrating the need for ISP compliance, e.g. the clean desk policy, are located all around the premises, thus employees are continually but discreetly reminded of the need to form the appropriate security behaviour as well as the underlying consequences of not being security-conscious (the simple use of the caption). This message appears to be conveyed successfully and employees adopt such practices as a matter of *habit*. Observation of employees' desks indicates that a clean policy is respected. Employees log off from their computers and do not leave their personal devices and belongings unattended.

7.3.2.2 Security Awareness

Special 'info sessions', which are seminars to inform employees about security threats and vulnerabilities, take place on a quarterly basis. During these seminars employees are informed of security issues and tools and raise their security *awareness*.

A noteworthy observation is that in addition to seminars, employees of the IT security department participate in security-related conferences, becoming aware of the latest trends and attacks in information security.

7.3.2.3 Perceptions about the cost of compliance

In order to minimise the *cost of compliance*, security managers of this organisation improve ISPs by making them user-friendly (e.g. use of clear *language*) and asking for employees' feedback and views.

7.3.3 Practices based on Technological factors

7.3.3.1 Usability

The antivirus tool is centrally configured for all computers. Every day automated checks for viruses are executed. There is minimum intervention with the antivirus, and thus this makes it usable for users.

In terms of *accessibility*, the organisation selects software suitable for people with disabilities. Employees with disabilities pre-test software to determine whether it is usable. This indicates the organisation's concern about the usability of its tools and interest in ensuring that employees with disabilities can *access* the appropriate software.

7.4 Recommendations for the enhancement of security management practices

The majority of the organisations' security management practices are effective. However, some shortcomings were also identified. Knowledge gained from literature provides further insights. Thus, the following section offers suggestions based on research findings which may be applied to supplement and enhance current information security practices and address the following shortcomings.

7.4.1 Establishing a Facilitating Organisational Environment

The organisation provides a number of resources to promote information security, e.g. training documents, seminars, posters, cards, etc. This approach reflects the organisation's

general policy of giving employees the opportunity to take responsibility for their own work and behaviour, and observation indicates this practice is successful. However, it is possible that a few employees may not respond appropriately to the information supplied- for example, some employees might not pick up one of the cards and captions, or may not pay much attention to the posters on display. One suggestion would be for security managers to send the relevant material to users individually, conveying the message more reliably that information security is critical and motivating them to form the appropriate security behaviour.

7.4.2 Engaging Management's Involvement and Compliance

The organisation has a clearly hierarchical organisational structure, being organised into Departments, with every department having its own Director. Every department is further divided into Units supervised by the appropriate management personnel. Top management plays a significant role in the way that departments operate as employees conform to the directions of their superiors and to the guidelines of the Director, regularly consulting their superiors on work-related decisions.

As in any large organisation, top management is not so visible, and it is difficult for employees to see their involvement in security-related issues. As this organisation is one where employees appear to follow the advice, instructions and behaviour of superiors, this would suggest that top management has a highly influential role. Given this existing advantage, it is recommended that security managers exploit this influence more fully by actively engaging management towards complying with ISPs, e.g. by encrypting their emails, sending emails relevant to information security, and being encouraged to participate more in security-related meetings, training, seminars, etc. Consequently, top management will set employees a more visible example of good information security behaviour.

7.4.3 Promoting security knowledge through awareness and training programs

Training material is available on the intranet and training sessions take place for raising employees' awareness about security issues. While useful, this information may not be of a sufficiently practical nature to guarantee that all employees both assimilate it and know how to deal with such security issues. Thus, hands-on training should also be provided to educate all employees on how to use security technologies and the consequences of failing to use them (Dinev & Hu, 2007). During security seminars, it is equally important to inform employees of the limitations of security tools so that they do not overestimate their effectiveness (Zhang et

al., 2009). As reported in literature, if there is an antivirus installed on users' computers, they might believe that their computers are protected and be less security cautious when browsing online or opening emails (Zhang et al., 2009). Additionally, special leave could be given to employees who participate in security-related trainings, thus acting as an incentive towards employees attending such events.

Aside from training another important aspect that literature suggests is the need for security managers to consider employees' confidence in following ISPs (Siponen et al., 2006; Herath & Rao, 2009; Vance et al., 2012; Ifinedo, 2012; Siponen et al., 2014). Although this organisation places emphasis on employees taking responsibility for their own security actions while at the same time strongly encouraging communication and support among colleagues and between employees and superiors, some employees may lack confidence in their ability to deal with certain security tasks. Thus, it is recommended that the organisation optimise opportunities for employees to gain the relevant skills and knowledge as well as assess their level of competence through self-assessment tests and simulations of IS attacks.

7.4.4 Designing and Implementing ISPs, Security Practices and Controls

7.4.4.1 Assigning Roles and Responsibilities

The organisation has assigned roles in every department, which has its own IT Department and the IT administrator is also assigned the role of Local Information Security Officer. In some cases, however, employees do not seem fully aware of this specific role. Security managers can rectify this by regularly communicating to employees the existence of certain security positions and responsibilities regarding ISP compliance. This can be achieved during training, seminars and meetings organised by the Local Information Security Officers of each Department.

7.4.4.2 Applying Rewards

Currently the organisation does not offer specific rewards for employee compliance, perhaps due to the fact that current security management standards like ISO 27001 do not stipulate what sanctions or rewards should be implemented. However, given the benefits of a reward system (Bulgurcu et al. 2010), when an employee identifies a security breach such as a phishing fraud and duly reports it to security personnel, he/she could receive a "thank you"

email that would also be sent to his/her superiors. This would reflect the organisation's emphasis on positive behaviours and makes employees feel valued.

7.4.4.3 Applying Monitoring Controls

To enhance compliance, except for log inspection it is recommended that Local Information Security Officers perform informal walk-in checks throughout the premises to see whether employees are following ISPs. For example, their inspection could check whether employees write their computer passwords on post-its and leave them in visible places, or whether they properly lock their laptops with special locks or keep them in a secure place when they leave them unattended.

7.4.5 Accommodating Individual Characteristics, Values and Habits

While literature suggests that security managers could employ targeted training methods for specific individual characteristics e.g. age or gender (D'Arcy and Greene, 2014; Ifinedo, 2014), this does not seem an appropriate practice for this organisation, which promotes equality as well as mutual respect among different nationalities. On the other hand, when communicating ISPs, security managers could pass on the message that ISPs should be followed by everyone, from top management to ordinary employees.

Current practices~~,~~ such as security-related posters or cards on stands promote ISP compliance out of habit. In addition to this, security managers could allocate a specific time in employees' daily work schedules to carry out security tasks, so as to further foster the practice of following them out of habit (Topa & Karyda, 2016).

7.4.6 Selecting and Implementing Appropriate Security Controls

The organisation's philosophy of equality extends to installing software that is accessible to all employees, including those with disabilities. Disabled people test software to ensure its compatibility with their needs. This philosophy of accessibility to all could be extended to security tools.

7.4.7 Leveraging Social Influence and Promoting Security Communication

Since employees of this organisation communicate with each other closely on a daily basis and in various ways, it is likely that they are influenced by their colleagues' actions and expectations (Herath & Rao, 2009a). Security managers could exploit employees' social influence and interaction more fully by encouraging Local Information Security Officers to communicate more regularly with employees and inform them about information security issues (e.g. security incidents).

Guidelines	Recommendations	Practical insights
Establishing a Facilitating Organisational Environment	Communication of material to employees. Checking assimilation of knowledge.	
Engaging Management's Involvement and Compliance	More visible top management security actions.	
Promotion of security knowledge through more awareness and training programs	More hands-on training. Regular self-assessment tests and simulations of IS attacks.	Attendance at information security conferences by IS employees. Provision of material for teleworkers.
Assigning Roles and Responsibilities	Raising awareness about the role of Local Information Security Officers.	
Applying Sanctions and Rewards	Reward mechanism for ISP compliant and good security behaviour.	Values and culture of organisation render sanctions unsuitable.
Applying Monitoring Controls and Mechanisms	Adoption of walk-in checks.	
Accommodating Individual	Greater emphasis on ISPs being followed by everyone, from top	Use of security-related posters and cards to subtly instil good security habits.

Characteristics, Values and Habits	management to ordinary employees. Allocation of specific time in daily schedules for security tasks.	
Selecting and Implementing Appropriate Security Controls	Accessibility of security tools for disabled people	
Leveraging Social Influence and Promoting Security Communication	More regular meetings and seminars in every department to raise employee awareness.	Knowledge sharing between experienced IT staff and less experienced employees.

Table 5: Recommendations and practical insights

7.5 Conclusions

This organisation has implemented several information security management practices successfully. Security managers keep up with the rapid changes in IT, e.g. the shift from the traditional workplace to a flexible way of working. Furthermore, they realise that ISPs need to be user-friendly and adopt a variety of different practices that motivate users to comply with ISPs.

More specifically, security managers have developed an effective facilitating organisational environment, providing adequate resources to employees. Apart from the purely organisational aspects, this organisation has implemented practices that address individual aspects, such as minimising cost of compliance, considering employees' values, characteristics, perceptions about risks and capabilities, security awareness, habits and experience. This organisation also addresses technological aspects such as accessibility of tools for people with disabilities.

This Thesis makes recommendations for improving current security management practices of this organisation. It is suggested that security managers could introduce rewards for employees who show good security behaviour, make top management's compliance more visible, promote security communication, raise employees' awareness about the role of Local

Information Security Officers, employ hands on training and adopt security tools that are accessible for people with disabilities.

The Technological-Organisational-Individual framework that is introduced in this Thesis aims to inform security managers about the various aspects that influence employee security behaviour. In order to achieve optimal security behaviour from their employees, security managers should apply those security management practices that are relevant to their type of organisation-in terms of size, purpose, values etc- and tailor their practices to suit the needs of their particular organisation. For example, while rewards could be implemented in this organisation, sanctions for non-compliance might not be an effective practice due to the nature of the organisation itself and its values.

Furthermore, it was identified that the organisational culture of the large organisation promotes communication, knowledge sharing, values and embraces employees' feedback. Such an organisational culture fosters an effective environment for employees to share their views about information security with colleagues and IT security experts and to help each other if they encounter difficulties in terms of information security. Furthermore, through the provision of security related material in the form of cards, posters and info sessions, employees are reminded of the need to comply with the ISPs and are encourages to comply with ISPs out of habit (e.g. by following the appropriate clean desk policy that is depicted on the cards). Therefore, security managers in this organisation by implementing the above security management practices instil employees the appropriate organisational information security culture (Karyda, 2017; Thomson et al., 2006) which leads to their ISP compliance.

The study of the information security management practices of this organisation shows important insights, which can serve as an example for other large organisations. Due to the size of the organisation as well as work and time constraints, it was not possible to extend the research to all members of the organisation. Though this limits the present case study, this organisation has a strong organisational culture and it is therefore likely that the general security management practices of the whole organisation are quite uniform and would not differ widely among departments. This case study concerns only one type of organisation, namely a large, international institution. However, the case study shows that when applying security management practices, organisations should not adopt a 'one-size-fits-all' approach by simply following all generally accepted standards; rather, they must pinpoint those practices that are most effective for their particular type of organisation in terms of size, purpose, values etc, tailor their practices to suit their organisation's needs and fully exploit their key strengths.

While security management standards such as ISO/IEC 27000 series (ISO/IEC 27001, 2013) make reference to the application of sanctions for ISP non-compliance, there are no

specific sanctions implemented in this organisation. The culture of this organisation can explain why it does not apply any form of sanctions, since the concept of punishment for poor security behaviour might contradict its values. Nevertheless, this case study also proposes that it could exploit one of its key strengths more fully with the addition of a reward system, confirming that individual employees who exhibit exceptional security behaviour are recognised and rewarded.

Moreover, for practical reasons it was not feasible to study certain technological factors in detail. The present study is therefore limited to a more general view, noting the organisation's awareness of technological issues such as ensuring software is accessible for people with disabilities or that new policies are written in easily understandable language.

Security managers need to bear in mind that it can take time to establish some of the previously mentioned security management practices. It can also take time for some ISPs to reach every part of the organisation and become standard practice.

Chapter 8: Guidelines for enhanced security management practices

8.1 Introduction

Based on the Technological-Organisational-Individual framework presented in chapter 5, on the gap analysis findings presented in chapter 6 and on the findings derived from the case study in chapter 7, the following section provides recommendations to security managers about the information security management practices they need to consider improving ISP compliance.

8.2 Guidelines addressing organisational, individual and technological aspects.

After conducting the gap analysis in chapter 6, it was identified that many of the factors of the framework were not adequately covered or not covered at all at the ISO 27001, 27002, 27003 and 27005. These factors include individual characteristics, values, habits, perceptions about capabilities, risks, costs and benefits, the cultural context, top management participation, social influence and usability factors. This implies that current security management practices lack important insights about the factors shaping security behaviour which were introduced in the framework in chapter 5. To address this gap and to inform security managers on how to exploit the factors of the framework a set of guidelines was introduced. These guidelines are mainly based on the guidelines of the ISO 27001, 27002, 27003, 27005 enriched with guidelines addressing additional factors of the Technological-Organisational-Individual framework. By following these guidelines security managers can adopt a comprehensive approach to security behaviour (Figure 16) and achieve better ISP compliance.

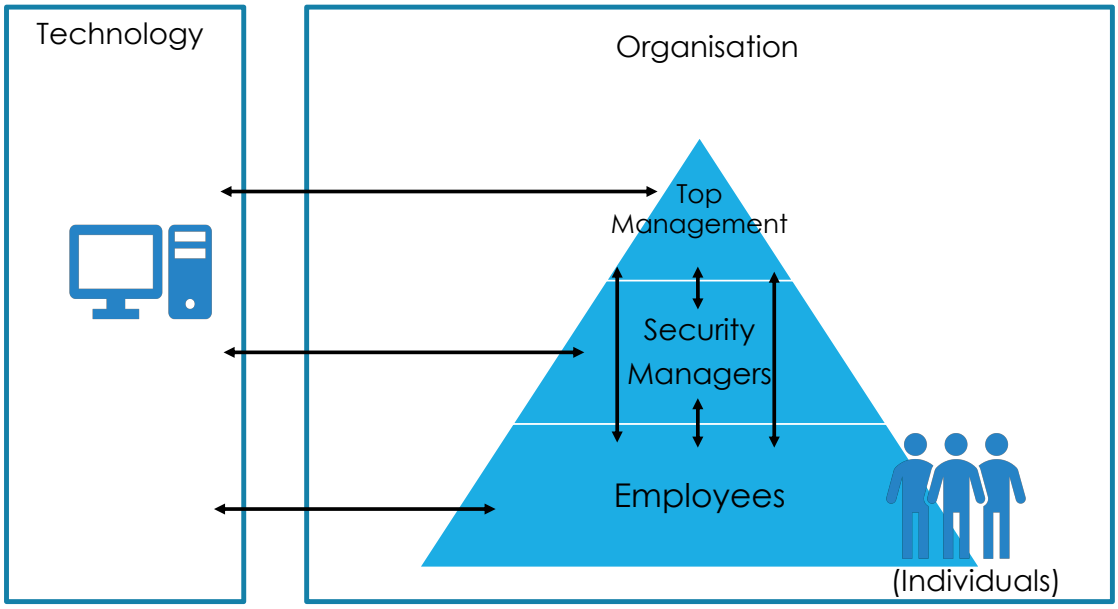

Figure 16: Comprehensive approach to security behaviour

8.2.1 Organisational aspects

8.2.1.1 Considering the role of organisational and national cultural context

It is important for security managers to take account of the particular national culture of employees since this affects their behaviour and their response to the different ways in which security issues are addressed. In a collectivistic national context, security managers could employ a group approach to training and raising awareness for security issues and tools, because individuals are motivated to use security tools by peers and superiors (Dinev et al., 2009). In collectivistic societies, employees act as a group and follow their colleagues' behaviour. From a positive perspective, this can lead to them adopting security tools collectively (Dinev et al., 2009). However, it may also result in employees breaking rules collectively (Connolly et al., 2015). For example, in an Irish financial organisation, when a manager requested access to restricted services and applications and the security manager granted him the corresponding authority, others followed suit, bypassing the security measure collectively (Connolly et al., 2015). In collectivistic societies, security managers need to engage people, especially those in managerial positions, to set a good example by following the appropriate security behaviour, and exploit group mentality to communicate the appropriate security behaviour to employees e.g. through meetings.

Conversely, in individualistic societies, security managers need to adopt methods such as sending emails, memos, using videos and generally encouraging employees as individuals to keep themselves informed. They could also provide online courses and individual self-paced

training to employees (Connolly et al., 2015). In individualistic cultures security managers may need to encourage employees to interact with each other and form groups so as to foster the appropriate security behaviour by organising team-building activities and outings, e.g. trips, sports, dinners, etc.

Security managers should bear in mind that in organisations with flat management, where employees' views are considered and not neglected, employees are motivated to follow ISPs as observed in the case study of this Thesis and in literature (Connolly et al., 2015). The case study above is an illustrative example of this type of management culture, where employees' views are valued, their input and feedback is sought and as a consequence there is a high level of ISP compliance.

8.2.1.2 Establishing a Facilitating Organisational Environment

Security managers need to need to provide employees with appropriate resources to foster ISP compliance. By creating an organisational environment that facilitates employees' appropriate security behaviour. Such resources can include training, effective communication practices (such as posters, newsletters and notices), ensuring that ISPs are easily accessible online or in different forms, help from experts and adequate time to become familiar with ISPs (Herath & Rao, 2009a; Safa et al., 2016; Pahnila et al., 2007). The provision of security education training and awareness programs could take various forms including classroom-based seminars, online courses, hands-on training and on-the-job training.

Various communication practices could be adopted to inform employees about information security. Security posters are an effective way of communicating the importance of being security conscious. This is an effective practice, which was reported in the case study in chapter 7. Large posters located in visible places convey clear and simple messages and effectively remind employees of the appropriate security behaviour.

ISPs need to be available in user-friendly form on the intranet and should be regularly updated. It is advisable to employ IT security experts (sometimes referred to as "champions") in every department of the organisation -depending on its size- so that employees can seek help whenever necessary.

The organisation should give some adjustment time to new employees to familiarise themselves with ISPs. Learning some new aspects of a security technology, such as changing the email password on different devices, might take time and practice. In the event that a new ISP is introduced, even experienced employees will need some time to become accustomed to any new security tasks which they will have to complete.

Apart from the provision of resources, security managers need to consider employees' level of job satisfaction, especially for non-IT employees and for employees in non-IT companies (D'Arcy & Greene, 2014). Job enrichment programs can enhance job satisfaction, while a working environment which promotes employees' satisfaction can not only enhance quality of work but also cultivate the right security behaviour (D'Arcy & Greene, 2014). In other words, satisfied employees are more compliant employees-hence the need for security managers to realise the benefits of establishing the right conditions for employee satisfaction.

Overall, research suggests that when employees' contribution is valued and they receive help whenever they need to, they are motivated to comply with ISPs (Shropshire et al., 2015). However, it is equally important to be aware of the potential dangers of the organisation being perceived as supportive. When there is strong organisational support in terms of information security, employees may mistakenly believe that security threats and breaches are primarily the responsibility of security personnel, rather than themselves, and not comprehend the importance of following ISPs, assuming the organisation can handle security problems even if they themselves should fail to comply (D'Arcy & Greene, 2014).

8.2.1.3 Engaging Management's Involvement and Compliance

Security behaviour can be influenced from the top down. Top management's active involvement in the creation, implementation and enforcement of ISPs can foster employees' perceptions that ISPs and procedures are legitimate and fair (Hu et al., 2012). Hence the need for security managers to encourage management's involvement. Security managers should therefore be aware that upper management needs to adopt security practices in a visible way, such as CEOs encrypting their emails and following ISPs (Hu et al., 2012). As it may be more difficult in large organisations for employees to see this kind of involvement, possible ways around this problem include top management's participation in security meetings and seminars and sending security-related emails. In very large or multi-national organisations, where staff may not have direct contact with those in top management positions, the security actions of employees' immediate superiors should be visible to them.

Top management should also take responsibility for security decisions, rather than assign the responsibility to lower level IT managers (Hu et al., 2012).

8.2.1.4 Promoting security awareness through SETA programs

It is essential that security managers be familiar with the many different types of awareness concerning security issues. Aside from ISP awareness, scholar research has

identified other types of awareness. These include general security awareness (security knowledge) (Bulgurcu et al., 2010), awareness of security tools and of the consequences of not using them (technology awareness) (Dinev & Hu, 2007), awareness of monitoring mechanisms and awareness of the content of SETA programs. (D'Arcy et al., 2009).

Regarding general security awareness, relative literature highlights the idea that individuals' perceptions about the effectiveness of their ISP compliant behaviour can make a difference (Herath & Rao, 2009a). Thus, security management should showcase instances where employees' behaviour has made an impact, whether positive or negative, e.g. an employee alerting the company to a threat or causing a security breach. Similarly, consequences to employees should be mentioned, i.e. rewards and sanctions (Bulgurcu et al., 2010).

Care is needed concerning the content and approach adopted in SETA programs to ensure that they are both appropriately informative and do not give employees a false sense of security. In simple terms, SETA programs should instruct individuals on how to use security technologies and inform them about the dangers of not using them (Dinev & Hu, 2007). Furthermore, they should present the effectiveness of the protection mechanisms without exaggeration, mentioning their limitations. In this way, employees can develop a more sophisticated and clearer awareness of security tools and of their own vital role in ensuring their effectiveness. Otherwise, when employees believe that there are high protection mechanisms already in place, they might become complacent and develop behaviours that are less security-conscious, such as opening email attachments coming from unauthorised sources on the assumption that an installed antivirus offers adequate protection (Zhang et al., 2009).

Security managers should foster greater awareness among employees of threats and vulnerabilities specific to their organisation (Ifinedo, 2012; Siponen et al., 2014) and the severity of these risks (Siponen et al., 2014, Herath & Rao, 2009a; Vance et al., 2012; Pahnila et al., 2013). Information deriving from risk assessments conducted in organisations are currently communicated only to security personnel and top management and not to all the employees. However, this information needs to be communicated to all employees. Providing employees with concrete examples of security threats relevant to their organisation enables them to realise that they are plausible and real. This can be achieved if SETA programs inform employees about security issues and incidents sourced from the news in the mass media and the internet (Siponen et al., 2006), but chosen particularly to reflect security issues their own organisation faces. More specifically, there could be online videos, in which employees speak about the cases that led to security breaches in one company. These scenarios can be real cases or fictional scenarios based on the most common security mistakes that employees make due

to ISP non-compliance. These videos can follow with employees explaining what were the consequences for the organisation tangible (e.g. fines, law violations) and intangible (e.g. loss of the company's reputation, etc.) and what is the appropriate security behaviour. Finally, self-assessment tests should follow. The above training material will make employees understand that security threats are real and if they try to avoid complying with ISPs, they will be reminded that they might cause security breaches and therefore be careful and develop the appropriate security behaviour. Extant literature provides a plethora of different methods for adopting when implementing security awareness programs to enhance security awareness (Tsohou et al., 2015a, 2015b). Security managers can identify those that best suit the needs of their organisation.

Another suggestion to enhance security awareness of employees is to encourage employees to participate in online tutorials about information security followed by self-assessment tests in order to raise money for a good cause, e.g. a charity, or a non-profit organisation. The more times employees will view the online material and complete the test the more money will be raised for the good cause.

An important consideration for security managers is how much emphasis should be given to raising awareness of threats. In other words, they need to tread a fine line between informing employees about security threats, so that employees feel motivated to comply, and placing excessive emphasis on security threats, which might intimidate employees, making them feel unable to deal with them (Pahnila et al., 2013).

8.2.1.5 Considering ISP Content, Availability and Communication

Security managers should appreciate the importance of a number of practical considerations regarding ISPs. To optimise ISPs' effectiveness, they should be of a reasonable size and written in clear language that is easy for employees to understand. Moreover, since information security is a constantly changing field, security managers need to ensure that all ISPs are updated regularly (Pahnila et al., 2007) and made available to all stakeholders both in printed or electronic form (Herath & Rao, 2009a). Clearly, employees can only adjust their security behaviour to suit new criteria if they are aware of and have access to any updates. Finally, it is important for security managers to ensure that any communication concerning ISPs is effective.

8.2.1.6 Assigning Roles and Responsibilities

One potentially dangerous 'grey area' in terms of information security may be that of roles and responsibilities. This might be due to due to different subcultures within organisations, a lack of effective communication or a failure to clearly assign specific responsibilities. Thus, when assigning and defining employees' roles and responsibilities regarding information security management need to establish clear boundaries and consider the different perceptions that may exist, as otherwise this may lead to conflicts. Kolkowska (2011) for instance, reports on a case where IT users relied on security personnel to provide them with information on how to protect organisational assets and secure networks and information, whereas the latter argued that employees ought to look for relevant information on their own and be responsible for protecting their own sensitive information. This highlights the importance of clearly designating security responsibilities to staff and ensuring that employees are aware of their duties.

8.2.1.7 Applying Sanctions and Rewards

The issue of sanctions for non-compliance is a complex one and requires careful handling by security managers, who need to be aware of the fact that research reports mixed findings on the effectiveness of sanctions for non-compliance. Some studies have found that sanctions do influence individuals' intention to comply with ISPs (Bulgurcu et al., 2010; Myyry et al., 2009), whereas others do not confirm such influence (Pahnila et al., 2007). An example of the latter might be the case study of the large organisation studied in chapter 7, where sanctions are not implemented, possibly as they would run counter to the organisation's commitment to creating a positive working environment and the general ethos of equality. Furthermore, there are studies reporting that in most cases severe punishment is less effective compared to the certainty of detection (Son, 2011; Herath & Rao, 2009a; Hearth & Rao, 2009b). This suggests that it may be more important for security managers to ensure that employees know their security behaviour is monitored rather than impose sanctions for violations. Given these conflicting findings, security managers should consider carefully whether adopting specific sanctions would be effective in their particular organisation. One suggestion for sanctions is to create "fake phishing emails" and send them to all employees. Those employees who click on the link, will have to attend an online tutorial about phishing and other security related issues. This practice is a light form of "sanction" which aims to improve security awareness of employees.

Turning to the role of rewards, security managers can and should adopt some form of reward system as literature suggests that employees are positively influenced. Individuals who believe that ISP compliance will lead to tangible and intangible rewards (e.g. pay raise, personal mention and appreciation in oral or in written reports, promotions and reputation) are motivated to follow ISPs (Bulgurcu et al. 2010). However, as is the case for other information security matters, to act as a strong security behaviour determinant, rewards need to be clearly articulated and well understood by employees, as in some researched cases employees reported that they were not aware of their existence (Pahnila et al., 2007; Siponen et al., 2014). Consequently, security managers need to specify the types of rewards that can be attained and ensure that employees are aware of them.

It is not common for organisations to offer financial rewards for ISP compliance. Other forms of rewards, however, should be provisioned. For instance, when an employee identifies a security breach such as a phishing fraud or an email containing a malicious virus, etc. which could harm the organisation severely and reports it in time to security personnel, he or she could receive a "thank you" email sent also to his/her superiors (Collett, 2015). This simple acknowledgement is likely to have a positive effect on the employee, especially since it will also make a good impression on his/her superiors.

8.2.1.8 Implementing Monitoring Controls and Mechanisms

As far as the implementation of monitoring controls is concerned, security managers should ideally adopt a combination of methods. The notion that monitoring is useful is not disputed as literature clearly documents that monitoring controls can deter employees from violating ISPs and emphasises that the existence and visibility of monitoring and detection mechanisms can be more effective for ISP compliance than the enforcement of severe punishments (Herath & Rao, 2009a; Herath & Rao, 2009b). Nevertheless, security managers are faced with a more complex task in view of practical obstacles. Since constant monitoring is typically difficult and expensive and activities such as noting down passwords cannot be easily monitored (Herath & Rao, 2009b), security managers need to adopt a mixture of security controls. This can be achieved by implementing a range of measures such as regular audit checks, informal walk-in checks and log inspection. Informal walk-in checks can include checks for post-its or notes of passwords on computer screens, under the keyboards, if laptops are locked when left unattended, if computers are in sleep mode when they are not in use, if employees are using privacy filters when handling sensitive information, etc.

8.2.1.9 Leveraging Social Influence and Promoting Security Communication

Security managers can exploit social aspects of their organisation to enhance ISP compliance. For example, they should encourage influential people, like the CISO, to communicate the importance of compliance with ISPs to employees (Ifinedo, 2012), who will be motivated by this type of influence from above. Research has also identified that one way in which employees become familiar with organisational values is through socialising with their co-workers (Ifinedo, 2014). More specifically, individuals are more likely to follow ISPs when ISP compliance is considered a social issue among their peers which will benefit the organisation and employees alike.

With this aim in mind, security managers need to encourage employees to participate in security-related meetings and form relationships with colleagues who share the same security views, so that they will be better motivated to comply with ISPs (Ifinedo, 2014). Similarly, security managers can ensure that employees engage in knowledge sharing, which can reduce training costs and enhance group mentality. However, security managers need to be aware of the different attitudes they may encounter regarding employees' willingness to share knowledge. According to Dinev & Hu (2007), individuals with an IT background tend to exchange views about security issues and tools, while basic IT users do not. Thus, as some employees may not be willing to share their knowledge, security managers need to encourage them e.g. by allocating a specific time in their working day to perform knowledge sharing or rewarding them with the incentive of additional leave. In the case study (chapter 7), it was identified that more experienced IT employees were willing to share their knowledge with less experienced employees due to the organisational culture which is based on communication and mutual support.

Another aspect of communication that security managers should encourage is incident reporting. Employees can be provided with a list of key security personnel to be contacted within reasonable time in case of a security incident.

8.2.2 Individual aspects

8.2.2.1 Accommodating Individual Characteristics, Values, Habits and Experience

Though highly complex, the influence of individual aspects on security behaviour cannot be ignored. Security managers need to create SETA programs which incorporate individual characteristics such as gender (Ifinedo, 2014) or age, since older employees tend to

comply with ISPs more than younger people (D'Arcy & Greene, 2014) and female employees have higher compliance intentions (Herath & Rao, 2009b; Ifinedo, 2014).

Security managers need to align ISPs with employees' values, so that their legitimacy is not questioned; moreover, this is more effective than sanctions (Son, 2011; Sommestad et al., 2014). Individuals who share organisational goals and values are better motivated to comply with ISPs (Son, 2011; Herath & Rao, 2009a). For instance, in an organisation where employees have a strong sense of loyalty, ISPs can be designed to show that ISP compliance is proof of loyal employee behaviour. Security managers can instil organisational values through employees' socialising with colleagues and perhaps through security training. Additionally, adopting a "pull" rather than "push" approach, by encouraging employees' participation in the ISP creation process and contribution to the security vision, rather than applying sanctions, will motivate them to follow ISPs (Sommestad et al., 2014; Chipperfield & Furnell, 2010).

Regarding those employees who display openness to change (Myyry et al., 2009) and those who feel their freedom is threatened by ISP compliance (Lowry & Moody, 2014), and thus react negatively to ISPs that restrict their access to the Internet or to other sources, security managers need to adopt a suitable approach such as convincing them of the effectiveness and necessity of security controls and promoting them in such a way as to turn these employees into allies.

When managers identify employees in key security roles who possess the above values, they could attenuate employees' ISP non-compliance, e.g. through promoting ISPs' legitimacy, training or monitoring. To bridge the gap between employees with different values, security managers could employ customised training and encourage them to internalise ISPs (Myyry et al., 2009).

In large organisations where security managers might have difficulty in identifying the values of the employees, they can create online questionnaires to gain information of the employees' values. These questionnaires should be anonymised and include a variety of values, from which employees will be asked to select the values they embrace, the values that are currently embraced by their team and the values that they would like their organisation to embrace. With these questionnaires security managers can gain a comprehensive understanding of the different values of the employees and try to align security policies with their values. They can also pass them the message that ISPs promote employees' values when they communicate ISPs. This is a good practice to be followed during seminars, by emails and during the induction seminars of new joiners, where they learn about the organisation and the way it operates.

Security managers need to encourage employees to comply with ISPs out of habits. One way to achieve this is to incorporate security tasks into work practices (Topa & Karyda, 2016), so that ISP compliance becomes ritualised and part of employees' work routine. Another suggestion is to allocate some time during employees' daily work schedule to carry out the security tasks. As a result, they will comply with ISPs automatically, without thinking that ISP compliance creates an impediment to their work. As it was further identified in the case study (chapter 7), the large organisation has stands with illustrated cards depicting a "bad" and a "good" clean desk policy practice. These cards show in one picture a desk with all devices left open and unattended and another picture with the same desk where the computer is in sleep mode and the devices are not visible. There is also a caption "Better safe than sorry". When employees see these cards in visible places, they are reminded of the importance to follow a good security behaviour and then this behaviour becomes a habit, as it was reported in the case study findings.

Experienced individuals are motivated to comply with ISPs (Safa et al., 2016). For critical positions employees with relevant experience in information security should be selected, because they can handle security breaches.

8.2.2.2 Minimising the Cost of Compliance

Cost of compliance can be attenuated by engaging users in the creation of ISPs, so that security managers receive feedback on employees' views and design ISPs that do not require significant additional effort or time (Kirlappos et al., 2015). Moreover, engaging employees in formulating ISPs can enhance employees' perceptions about the effectiveness of ISPs and lead them to ISP compliance (Siponen et al., 2014). ISO 27002:2013 (section 5.1.2) for reviewing ISPs also supports exploiting employees' feedback. Security managers can conduct usability reviews to evaluate their security management practices (Vance et al., 2012).

8.2.2.3 Perceptions about individual capabilities

Security managers should organise and encourage discussions to help employees feel confident in their abilities to follow ISPs (Siponen et al., 2006; Herath and Rao, 2009a; Vance et al., 2012; Ifinedo, 2012; Siponen et al., 2014). Security managers need to expose employees to emerging security technologies, cultivating the appropriate skills and knowledge (Ifinedo, 2012) and ensuring they have assimilated the knowledge through regular self-assessments and simulations of security attacks.

8.2.2.4 Perceptions regarding risks

Security managers need to be aware of individuals' perceptions about risks. They can achieve this if they create questionnaires and organise discussions to understand users' perceptions about the risks and threats. Through security awareness programs and security material, e.g. training documents, security managers can inform employees about security threats and risks.

8.2.3 Technological aspects

8.2.3.1 Selecting and implementing security tools

Typically, security managers select security controls in terms of effectiveness, cost and applicability, but related research provides further useful insights on what influences the use of security tools (Dinev and Hu, 2007; Herath et al., 2014; Payne and Edwards, 2008). Employees mainly use technologies and tools depending on how effective they consider them to be: e.g. Herath et al. (2014) found that users were more willing to use an email authentication service when they considered it effective in thwarting IS threats.

Security controls also need to be usable and user friendly (Herath et al., 2014; Payne and Edwards, 2008). Some usability characteristics that security can consider when deciding which security tools to implement are accessibility (security tools are available to users with disabilities), language (security tools have language that easy to understand, e.g. without including many technical terms) and intuitiveness (security tools' settings are easy to find, security tools include indicators showing users what is happening in terms of security, security tools are easy to learn and easy to understand how to be used) (Topa & Karyda, 2018).

Feedback and errors (security tools provide feedback messages to users and messages about errors), error prevention (security tools prevent users from making errors) and undo of actions (security tools allow users to undo their actions) are some more usability factors. Another usability factor is efficiency (security tools are efficient in use without time delays) which includes responsiveness (security tools have little response time and users do not have to wait long for the security processes to be performed).

Other usability characteristics that security managers could take into account are minimalistic design (security tools show only the relevant information and follow modern trends), consistency (security tools follow a consistent form e.g. after updates) and availability

of information and support (security tools have available help and support). Employees use various devices and therefore availability of tools among various platforms (security tools are available among different operating systems and platforms) is a usability factor that should be considered by security managers (Topa & Karyda, 2018). They should have security tools available not only for computers but for the employees' portable devices.

Automation is another usability characteristic that security managers can consider when selecting security tools, as it is easier for users to use tools correctly if processes are automated and there is limited control over the tool (Topa & Karyda, 2018). However, in the case of BYOD, some users might prefer control over automation (security tools offer users the opportunity to configure the security settings themselves or they give limited control and the processes are automated) (Topa & Karyda, 2018).

For users who use organisational portable devices or their own personal devices for teleworking purposes, usability characteristics relevant to installation need to be considered (Topa & Karyda, 2018). Such usability characteristics are easy installation process, avoid registering with personal data for ease of use, minimum requirements of the operating system are visible, small changes occur upon installation.

Privacy characteristics such as transparency and control of users' data can be considered for users' who are concerned about their privacy (Topa & Karyda, 2018). Privacy concerns stemming from the use of a security technology or service, e.g. an email authentication service, may deter individuals from using it, because the tool may gather, retain and use personal information such as email recipients (Herath et al., 2014). Security managers should, therefore, inform employees about the privacy policies of the security tools while simultaneously identify their employees' privacy concerns through interviews or questionnaires. In cases where employees have major privacy concerns, alternative security tools could be implemented.

8.3 Conclusions

Based on the factors that are included in the Technological-Organisational-Individual framework (chapter 5) security management can benefit if security managers incorporate these factors in their security practices.

Security managers are provided with a set of guidelines that address all three categories of factors, namely organisational, individual and technological. It is important that security managers address all three categories of factors when implementing their security management practices. As a result, they can have a comprehensive approach to the security behaviour of

employees and implement practices that will lead to ISP compliance. Security managers need to study the context of their organisations and create strategies that best suit their organisation.

For some factors, it is not easy to provide definite guidelines, for example in the case of sanctions. However there are presented alternative guidelines that might be more effective than sanctions, e.g. implementing monitoring controls, embracing employees' feedback when designing ISPs policies, etc.

Individual related aspects, such as perceptions about capabilities and values, might be challenging for security managers to consider during the implementation of their security management practices. However, guidelines in this section help security managers to get an understanding of how to address them even if they are not familiar with them. Finally, this set of guidelines, provides security managers with supplementary knowledge and by addressing all three categories of factors they can create a security culture which will benefit the organisation in the long term (Schein, 2010; Connolly, 2015).

Chapter 9: Discussion

9.1 Introduction

For the Research Questions of this Thesis a discussion of the findings is provided in this chapter. To address the research questions different research methods were employed, including a comprehensive literature review, a survey on the usability of security and privacy tools, a gap analysis regarding ISO Standards 27001, 27002, 27003 and 27005 and finally a case study on a large organisation. Drawing on the findings of the above stages in the research phase of this Thesis, a Technological-Organisational-Individual framework and a set of guidelines were created to provide security managers with a comprehensive understanding of the factors shaping security behaviour and to act as a roadmap to assist them in designing security management practices that will lead to improved employee ISP compliance. In the following section there is a discussion of the methods used, of the findings of this Thesis and their contribution to the field of security behaviour. There is reference to the practical implications of the findings to security managers, developers and designers of security tools. Furthermore, implications of this Thesis to theory are also described, some of which include the introduction of the Technological-Organisational-Individual framework, the investigation of the role of technology and the identification of usability characteristics of security and privacy tools that are significant to users, the analysis of security management practices followed to support employees who are teleworking etc. Finally, the limitations of this Thesis and reflections on possible future research are stated.

9.2 Security Behaviour and ISP Compliance: From Theory to Practice

9.2.1 Discussion of Findings

To answer the first research question of this Thesis all the factors involved in information security behaviour were identified. This Thesis has shown that although there is a wealth of literature concerning the multitude of factors that determine security behaviour, much of the valuable information that literature has to offer is not accessible to security managers. This can be attributed to a variety of reasons. Firstly, the sheer volume of information available is difficult to assimilate. Added to this is the fact that it is not all compiled in one body of knowledge which security managers can access. The terminology may also be complicated

with confusing terms such as self-efficacy, preconventional moral reasoning, perceived value congruence, while similar concepts may be introduced under different terms, as in the case of resource availability and facilitating conditions. Furthermore, a deep understanding of certain concepts which draw on theories such as the Theory of Reasoned Action, General Deterrence Theory, Rational Choice Theory, etc. would require advanced knowledge on the part of security managers and may appear too demanding. Finally, for purely practical reasons, such as time limitations or limited resources, security managers would almost certainly have difficulty in analysing all the important research findings related to security behaviour. Thus, it seems even less unlikely that security managers could exploit these insights in their security management practices.

On the other hand, this Thesis has also shown that the ISO Standards 27001, 27002, 27003 and 27005, which are extensively applied in security management, are generic in scope. While they provide organisations with guidelines for the functional and non-functional requirements in systems' design and architecture (Tsohou et al., 2010), these guidelines must, by their nature, be general, since they need to be applicable in all organisations worldwide and consequently do not offer concrete examples or specific practical steps to follow. A case in point would be that there is no reference to the different types of rewards or sanctions that can be implemented in the organisations. This poses a challenge to security managers who must design security management practices based on their understanding of these generic guidelines, which they may find vague or unclear. In addition, although this Thesis has highlighted the importance of individual characteristics as security behaviour determinants, the above ISO Standards do not deal with individual aspects. Thus, if security managers confine their security management awareness solely to guidelines described in ISO 27001, 27002, 27003 and 27005, they will not be able to form a fully comprehensive view of security behaviour.

While there is reference to the technological factors influencing security behaviour in the literature of security behaviour (Dinev and Hu, 2007), the role of technology and the usability characteristics of security tools from the users' perspective in particular are not adequately investigated (Topa & Karyda, 2018). Through a survey conducted in this Thesis, a broad spectrum of usability characteristics of security and privacy tools was identified. Individuals want security tools to accommodate a variety of usability characteristics so that they find security settings easily without spending too much time, they understand how to use the tools and carry out the security tasks easily, the tools are efficient without imposing time delays, etc. One interesting finding of this survey was that the characteristic of control was found as important by users. However, some users preferred automation of processes achieved for example through the use of machine learning and advanced algorithms. This can be

attributed to the fact that participants of this survey were experienced ICT users who are used to configuring the settings of the tools and are more aware about the tool's technical functionalities. However, in practice normal users might not be familiar with the configuration settings of security tools. One suggestion would be that developers implement different settings for basic and advanced users. The benefits of making security "frictionless" have been discussed in literature (Furnell, 2016; Cranor & Buchler, 2014). As a result, employing "smart defaults" (Cranor & Buchler, 2014), artificial intelligence algorithms, embedding security into design and developing automated security tools that require only limited interaction with the users should be an area of further research.

Through this survey, users reported that there is a trade-off between security and usability, e.g. in Tor, in case of high security the usability is low (videos and pictures are not displayed, the browser is slow) while on the contrary when security is limited, usability is high. Literature has long ago described the discrepancies between security and usability (Whitten & Tygar, 1999). This Thesis can help security developers to bridge the gap between security and usability through the identification of usability characteristics that are important to users. Designers can benefit if they implement these characteristics in practice to design security and privacy tools that are usable, intuitive and efficient.

It is important to mention that this Thesis has considered the modern practice of teleworking that is being adopted widely by organisations and thus some of the usability characteristics investigated are suitable for employees who telework and they are responsible for securing their personal devices in case of Bring your Own Device or the company's devices. Furthermore, this survey also sheds light on the usability characteristics of privacy tools, which may be significant to users, particularly for employees who work in highly confidential positions or those who want to preserve their privacy when teleworking. In this case users are concerned about trust the control of their data and transparency in the way their data are processed.

To answer the second research question of this Thesis, namely how can the knowledge of the factors identified in literature be exploited to assist security managers in enhancing their security management practices, this Thesis developed a framework of security behaviour factors. The factors incorporated in the framework are drawn from literature but classified according to three categories and employing similar language to that found in ISO 27001, 27002, 27003 and 27005 to facilitate better understanding. One important objective in devising the framework was to design it in such a way that it would be user-friendly for security managers. Hence the choice of terms security managers would generally be familiar with and the classification of security behaviour factors in a clear, accessible form.

Nevertheless, one of the key issues security managers need to be aware of is that security behaviour factors tend to be interconnected and interdependent. For example, security awareness, while it constitutes an individual factor, requires the intervention of the organisation. In other words, it is the organisation that must provide appropriate training and resources to cultivate an individual employee's awareness. Furthermore, security awareness is also connected with technological factors, since, for instance, the more user-friendly the tool is, the more easily the individual will develop security awareness of the specific tool. Conversely, if a particular security tool demands too much time or effort on the part of the employee, this will affect the user's perceptions concerning cost of compliance. This interconnectedness and interdependence of the various security behaviour factors represents a challenge for security managers. For this reason, this Thesis, provides also a case study and practical guidelines, to facilitate security managers and help them understand how to implement the framework in practice. Furthermore, this framework assists security managers in adopting a more comprehensive approach when designing and implementing their security management practices, as it will encourage them to view all three categories of factors- individual, organisational and technological- as integral parts of security management.

To test the applicability of the above framework, a case study was conducted in a large public sector organisation in chapter 7. It was identified that this organisation addressed a plethora of factors stated in the framework which was analysed in chapter 5. The case study revealed that this large organisation follows certain good security practices, e.g. updating security polices regularly, writing ISPs in a user-friendly way, considering employees' views and try to minimise the cost of compliance. It is important to mention that security managers of this organisation have realised that employees can make a difference in Information Security when complying with ISPs. This is why they address individual factors in their security management practices and find ways to motivate employees comply with ISPs, and avoid potential security risks and breaches. Security managers are interested in making employees accountable for information security and facilitate them to form an appropriate security behaviour. They are also concerned about the new trend of teleworking that was recently introduced in the organisation. To avoid potential security breaches security managers prepared a new teleworking policy that aims to inform employees about security threats, risks and what actions and security countermeasures they need to take when teleworking. As a result they put a lot of emphasis on individual's perceptions about risks and address them by providing material to raise their awareness and encourage them form the appropriate security behaviour.

Other reasons why this organisation follows good practices is because a wreath of the information managed is confidential and there is a need to protect the information assets of the

organisation from security threats and attacks. Furthermore, a large budget is invested yearly for the implementation of security management practices and security controls. Furthermore, a considerable number of security managers and experienced employees working for IT security. However, the reality might be different in smaller private companies, as the IT security personnel is limited in number and there might not be any IT security experts. As a result, IT administrators are responsible for IT security. In this case the employee who acts as a security manager might not have the time and knowledge to deal with all the security aspects successfully which might lead to ineffective security management practices. For example, ISPs might be reviewed regularly. Security managers need to make sure that ISPs are reviewed and updated regularly, at least once a year. Sometimes, ISPs are an exact copy of the ISO Standards and therefore they are too generic to employees, e.g. there may be reference to sanctions, but no information on what these sanctions are and when they are enforced. In some cases, organisations do not have separate ISPs for employees, but have one document, which is broader in scope and is called handbook. Handbooks contain information that is relevant for IT security employees and IT administrators rather than ordinary users, making it difficult for non-IT personnel to understand them or to identify which information is relevant to their role and responsibilities.

According to relevant literature, fostering an information security culture in organisations can be challenging for security managers (Karyda, 2017). In the case study analysed in chapter 7, it was identified that the organisational culture of the large organisation promotes communication, knowledge sharing, values and embraces employees' feedback. Such an organisational culture fosters an effective environment for employees to share their views about information security with colleagues and IT security experts and to help each other if they encounter difficulties in terms of information security. Furthermore, through the provision of security related material in the form of cards, posters and info sessions, employees are reminded of the need to comply with the ISPs and are encourages to comply with ISPs out of habit (e.g. by following the appropriate clean desk policy that is depicted on the cards). Therefore, this organisation has implemented such security management practices that instil employees the appropriate organisational information security culture which motivates them to comply with ISPs. This is an important finding, as it shows that security manager by considering all aspects of the framework and implementing the appropriate security management practices, they are able to promote an information organizational culture according to which employees.

Apart from the good security management practices identified in the organisation of the case study there were some shortcomings. These were relevant to the fact that not all employees

were aware of the role of the Local Information Security Officer, only a few info sessions take place to raise employees' security awareness, no sanctions of rewards are implemented, usability in terms of security tools was not identified. To address these shortcomings, additional recommendations were provided which can supplement current security managements towards enhancing ISP compliance. One of the recommendations was that this particular organisation has such an organizational security culture that would benefit from adopting a rewarding system rather than imposing sanctions.

To adequately address the second research question of this Thesis and identify how the knowledge of factors influencing security behaviour can be exploited by security managers to enhance their security management practices, a study of current literature was conducted. While literature presents a plethora of factors influencing security behaviour, there is little reference of these factors' practical implications. The majority of scientific papers highlight which factors impact security behaviour, however they provide only limited guidance for security managers on how to exploit these factors. For example in the case of individuals' values (perceived legitimacy and perceived value congruence), it is suggested that security managers should align employees' values with the ISPs, but this is not explained in detail how security managers can achieve this.

Furthermore, an analysis of current security management standards was conducted to identify the security management practices which are currently followed. To determine whether the widely used ISO 27001, 27002, 27003 and 27005 incorporate the factors influencing security behaviour forming the framework described in chapter 6, a gap analysis was carried out. As a result, some factors including the cultural context, top management participation, individual aspects, values and perceptions about capabilities, risks, costs and benefits, were not addressed. To bridge the gap, between theory and practice and to facilitate security managers with practical insights they can follow to supplement the directions of ISO 27001, 27002, 27003 and 27005, a set of practical guidelines was developed and presented in chapter 8.

For some factors of the framework it was not possible to provide explicit practical guidelines because literature findings are contradictory or unclear: for example, there were identified conflicting implications with regard to sanctions and rewards (Bulgurcu et al., 2010; Son, 2011, D'Arcy et al., 2009). In some studies, sanctions are security behaviour determinants (Bulgurcu et al., 2010) while in others they are not (Son, 2011, D'Arcy et al., 2009). The effectiveness of sanctions has been discussed among researchers and mixed results were identified (Topa & Karyda, 2019; D'Arcy and Herath 2011). This can be attributed to many factors, for example due to the different way that research was carried out (for example the

definition of the factors for measuring sanctions varies among research, perceptions of sanctions might vary among people with different IT skills, among employees who are woking at the office and those who telework, etc.) (D'Arcy and Herath 2011); because it is not common for some organisations to apply sanctions to those employees who do not perform certain security actions, e.g. locking their computers, sharing their passwords and following insecure USB practices (Moody et al., 2018). Therefore, more research is needed in the field of sanctions and rewards.

Furthermore, other researchers argue that sanctions are not effective, and other approaches should be used instead (D'Arcy et al. 2009; Herath & Rao 2009a; Siponen & Vance 2012; Theoharidou et al. 2005). To accommodate the discrepancies found in literature security managers can adopt different alternatives, e.g. options which have been identified as more effective than using sanctions, such as using and implementing monitoring controls and measures (Herath & Rao 2009a), embracing the employees in the decision-making process, promoting ISPs as legitimate or aligning ISPs with employees' values, creating a security culture. For example, in an organisation with an organisational culture with promotes communication and mutual support, sanctions might not be an effective practice for ISP compliance, as identified in the case study presented in chapter 7. On the other hand, employing a rewarding mechanism, e.g. send a "thank you email" to show that employees' contribution is valued when they identify a malicious phishing email and report it to the IT Security personnel can be more effective than implementing sanctions.

It is important to highlight that the guidelines are interconnected and can be combined. For example, cultural aspects can be related to training programs. More specifically, in collectivistic countries, there should be seminars for group-based trainings, while for individualistic countries such as the USA, there should be training courses through an online platform or training videos targeted for individuals. Training can also be related to social influence and communication which exist throughout the organisation, e.g. in an organisation which is based on communication such as the organisation analysed in the case study (chapter 7), info sessions take place to inform employees about information security. However, in organisations that promotes competition among employees, the use of individual training videos and self-assessment tests will be employed instead.

To help security managers understand how to design and implement security management practices presented in chapter 8, it is suggested that they follow two basic steps:

1. First security managers should understand the context of their organisation, its security requirements and needs. For example, a nuclear factory or a hospital will have different ISPs and ISP compliance requirements from a manufacturing company. Furthermore, as far as

the context of the organisation is concerned, if the organisation is a non IT-company, then dealing with employees working in such a company, who are likely to be less experienced in IT procedures, might pose a challenge. However as suggested in chapter 8, other factors should be highlighted in this case, e.g. the organisation should make the employee's job satisfaction, so that the employee will be satisfied with his/her job and is willing to comply with ISPs.

2. Second they need to identify the key strengths of the organisation and customize their security management practices accordingly. For example, in the case study analysed in chapter 7 it was identified that the organisations' key strengths are communication and top management influence. As a result, security managers can benefit from these key strengths and design their security management accordingly. Security managers already ask for employee's feedback. They can further benefit if they encourage the LISO's to organise seminars and events to inform about security issues and if they encourage top management to actively participate in promoting information security through emails, talks, newsletter and following the appropriate security behaviour in a way that is visible to employees.

It is of vital importance that security managers understand that there is no one-size-fit-all approach towards implementing the set of practical guidelines analysed in chapter 8. They need to design their strategy towards implementing security management practices in such a way that is customised to meet their organisation's security requirements and needs and to exploit its key strengths.

9.2.2 Challenges for Security Managers

Security managers are already familiar with some of the guidelines provided in chapter 8, especially those that are based on common and best practice, such as security awareness and training programs, selecting the appropriate security controls, monitoring and so on. However, there are also guidelines that might be challenging for the security managers to implement, they require considerable effort and time, appropriate soft skills and an awareness of all the factors that determine security behaviour. These include engaging top management in performing security actions, encouraging employees to comply with ISPs out of habit, formulating groups of employees to communicate and share security knowledge, encouraging employees to give feedback to IT security personnel, accommodating individual characteristics and values and embracing the national cultural context. These security management practices are long-term investments, require time to reach all parts of the organisation and become common practice and require the cooperation and involvement of all stakeholders.

One challenging aspect for security managers is to align employees' perceptions about capabilities with the provision of organisational resources. For example, when providing organisational support security managers need to be aware of the fact that an overly supportive facilitating environment might lead employees to the misconception that the organisation is resilient, and that should they fail to safeguard organisational assets, security personnel will do it for them (D'Arcy and Greene, 2014). Thus, it is essential that security managers find the appropriate balance between providing adequate resources and ensuring that employees feel confident and responsible towards maintaining information security. Furthermore, part of the organisational support is the provision of training and awareness programs, as suggested in ISO Standards. However, a challenge that security managers might face is to ensure that all employees have assimilated the knowledge provided by these programs and that they have developed the necessary capabilities and confidence.

Security managers might face difficulties when implementing security management practices to an organisation that is located in multiple countries. In this case in every office of the organisation there is a different national cultural and therefore different security management practices should be adopted. For example, in a large organisation that is located in Europe, but has several offices around the world, e.g. in other European countries, in the U.S.A. and in Asia, employees will have different national cultures and security managers need to design their security management practices to suit the cultural needs of their employees.

Another challenge that security managers might face is employees' reluctance to comply with ISPs by bypassing security countermeasures out of a desire to be more productive and avoid impediments. It is thus possible that some organisations themselves value productivity over security, overlooking ISP non-compliance. In cases where a conflict of interest exists, the challenge for security managers is to convince all stakeholders, including upper management of the importance of ISP compliance. In the European Union where the Data Protection Regulation was imposed on May 2018 (Mitrou, 2017b; Karyda & Mitrou, 2016), organisations are concerned about security practices and ISP non-compliance implementing security countermeasures and promoting security awareness through seminars, trainings and videos. ISP compliance is needed because otherwise there will be severe consequences to the organisation, including fines, reputation loss, etc.

Finally, security managers are faced with the challenge to balance security and usability when designing their security management practices. This PhD Thesis through the survey conducted in chapter 4, highlights this need and proposes ways to achieve this balance, e.g. through the use of language that is easy to understand and it does not include many technical terms. However, with the advancement of technology, and the interconnectivity of systems,

networks and devices which have led to an increased number and complexity of security threats and vulnerabilities, security managers tend to implement strict security practices and select security tools, authentication mechanisms, teleworking techniques etc. that are not usable for ordinary users. Examples of this are: the requirement to change a password every 60 days; employees being given 5 attempts before Windows locking their accounts but needing an hour to retrieve the key and enter the Windows account; or the necessity of entering the email password every time before logging in to emails using a business smartphone. When it comes to teleworking, user access authentication using multi-factor authentication can be confusing, frustrating and time-consuming. More specifically, the user has to enter a one-time code (usually a 6-digit code) which is generated very quickly (e.g. every 30 seconds) along with a fixed passphrase (including e.g. the initials of the employee, the brand of the company and random numbers). Although literature suggests that practices, policies and security tools need to be user friendly, this is not always the case as is shown in the previous examples of real security practices. Therefore, security managers need to find a balance between security and usability in their practices and in implementing usable security tools. This PhD Thesis informs security managers on what actions they need to take to help them create and implement security management practices are usable for all employees.

9.3 Implications for practice

The framework provides a comprehensive view of technological, organisational and individual factors influencing security behaviour. The framework and the set of guidelines equip security managers with a roadmap on how to implement their security management practices in order to achieve enhanced ISP compliance. This roadmap is enriched with literature findings about security behaviour determinants and their implications, insights about the role of technology and of the usability characteristics of security and privacy tools and guidance on how to apply the above knowledge in practice. This is a significant contribution for security managers as security management practices that are described in ISO Standards 27001, 27002, 27003 and 27005 are generic in scope and do not incorporate useful insights from literature or any practical guidance about how to implement the recommended practices.

Literature postulates that security tools are not usable and that individuals fail to use them correctly for various reasons (Whitten and Tygar, 1999; Cranor & Buchler, 2014, Furnell 2010, 2016). In the survey of chapter 4 there were users who failed to use the security tools correctly. This confirms that security and privacy tools are not sufficiently usable and lead users to mistakes. Since it may be argued that better usability would result in fewer mistakes

as well as increased satisfaction, developers can benefit from the findings of this Thesis by gaining a comprehensive understanding of the usability characteristics that users value as important. Thus, they can consider these characteristics when designing security tools and develop usable security tools. The ultimate aim should be to implement usable security tools by design. Finally, it is important that vendors offering security tools need to invest in usable security tools and encourage research to be conducted in this field towards developing security tools that are usable. As a result, this will bridge the gap between the existence of a plethora of security tools and users' failure to use them correctly.

This Thesis addresses the challenges that arise from teleworking and the need for organisations to develop teleworking policies and encourage employees to comply with ISPs when teleworking. In the future teleworking might lead to a new form of "ISPs", as ISPs should be available in more user-friendly ways, e.g. in the form of videos, which employees who are teleworking will be motivated to watch. Perhaps there could be pop-up windows and reminders to inform employees that they need to watch training sessions about ISPs on a regular basis or complete a checklist with the security practices they follow to determine whether they are compliant e.g. to see whether they have installed antivirus, update the antivirus daily, scan their pc for viruses, use guest accounts for other users, and so on.

9.4 Implications for theory

This Thesis investigates the factors that motivate users to comply with ISPs and use security tools. While there are some frameworks in literature to address technology acceptance, at organizational level such as the Technological-Organisational-Environmental (TOE) and at individual level such as the Technological-Personal-Environmental (TPE) framework, these frameworks did not address all three categories of factors that were identified in this Thesis. The need to have a framework where all three categories of factors are included, namely technological, organisational and individual, led to the introduction of a new framework which is developed and analysed in this Thesis and can be named as Technological-Organisational-Individual (TOI) framework. As future research this framework could be further validated in practice in different types of organisations.

Currently there is research conducted by Nielsen (1994, 2005) into the usability characteristics of applications. However, there is little guidance about the usability characteristics of security and privacy tools. This Thesis adds to the current literature on usable security by identifying a broad spectrum of usability characteristics of security and privacy

tools that individual users regard as important, highlighting the user's perspective and revealing areas for improvement.

Looking to the future, developers and researchers can build on these findings to collaborate towards establishing principles for designing and implementing more usable security tools. The key contribution of the usability study to the field of security tools is the importance of aligning security and usability. There is also need for researchers to investigate usability beyond the user interface and identify ways to design usable security tools (Krol et al., 2016; Payne & Edwards, 2008). There is an area for future research in machine learning and artificial intelligence to identify ways to promote automation in order to limit the impediment caused by security (Cranor & Buchler, 2014).

Technological trends have introduced teleworking, as a modern way of working, in organisations. Literature studies are focused mainly on ISP compliance in the traditional workspace and there is limited research regarding the different factors influencing employees' intention to comply with ISPs when teleworking or when using their own devices. One study has investigated the factors that motivate users to secure their mobile devices (Garza & Guo, 2015). This is an area for further research as researchers should investigate in more detail the factors influencing teleworkers and those employees who are using their own devices to comply with ISPs and follow the appropriate security behaviour.

9.5 Limitations

Although current literature on ISP compliance and security behaviour provides useful information and insights the present Thesis found certain limitations concerning the information available. Some studies cited in this research measure the intention of employees to comply with ISPs and not actual compliance. Another limitation is that these studies do not measure continuous security behaviour. While there is literature on the continuance of security-related behaviours, such as the study of Warkentin et al. (2016), further research is needed in this field. Furthermore, ISP compliance is a broad term and can therefore refer to a variety of different actions, e.g. password-sharing, taking down passwords in post-its, using USB keys to store confidential information, opening spam emails, etc. While in some studies there is information about the specific aspects of ISP compliance that were tested, in others there is no clear picture about the practices relevant to ISP compliance that were being investigated. In these cases, studies refer to ISP compliance in general.

Regarding the research conducted in this Thesis, since the focus of this research is security behaviour and ISP compliance in organisations, the usability survey ideally should

have been conducted with employees. For practical reasons, however, this was not possible and thus the selection of participants for this survey was limited to undergraduate IT students. Nevertheless, this approach had certain advantages. The users were more technically experienced and thus competent in providing their views about the usability of the security and privacy tools. Moreover, the number of participants was considerable, 150 in total, whereas it might not have been feasible to gather 150 employees to participate in such a survey.

The tools which were used in the survey were one security tool (Malwarebytes) and two privacy tools (Tor and Ghostery). The results for the two different kinds of tools were similar and there were no significant discrepancies, with the only exception being in the case of privacy tools where users were concerned about the control of their personal data and transparency. However, it was not possible for practical reasons to include more security tools in this survey, as security tools such as antivirus are paid tools. Another limitation is that we assigned participants of the survey to use applications that were installed locally on their computers. It is common practice in organisations for administrators in the IT department to install security applications and configure the security settings. In the survey that was conducted participants were able to install the security and privacy tools and configure them on their own. This practice is aligned with the modern trend of teleworking and BYOD, according to which employees have portable devices, including their own personal devices and can download and install applications for work purposes, security and privacy tools. In the case of BYOD in particular, employees are responsible for securing their own devices. Therefore, this survey was carried out with individual users who were unattended, simulating the working conditions and environment of teleworkers.

Regarding the case study this large organisation, implements many security practices effectively because it has the budget to invest in information security. Due to the size of the organisation as well as work and time constraints, it was not possible to extend the research to all members of the organisation. Moreover, for practical reasons it was not feasible to study certain technological factors in detail. The present study is therefore limited to a more general view, noting the organisation's awareness of technological issues such as that of ensuring software is accessible for people with disabilities or that new policies are written in easily understandable language. However, the fact that this organisation is using software that is suitable for people with disabilities shows that it is concerned about the usability of tools and about finding ways to make its IT practices user-friendly.

9.6 Conclusions

The previous sections provide a discussion of the findings of this Thesis. The framework was created to bridge the gap between the knowledge of factors which influence security behaviour identified in literature and the security management practices described in ISO 27001, 27002, 27003 and 27005. A key point for discussion is that all factors are interconnected and interdependent with each other. The guidelines create further areas for discussion such as the fact that the literature findings are not explicit about certain aspects, e.g. rewards and sanctions. Certain security management practices might be easy for security managers to implement as they are common practices while others might be more challenging and demand time, e.g. addressing individuals' values. To achieve these more complex, long-term goals of security management, security managers should aim to create a security culture. The Thesis also highlights what security managers should do prior to implementing their security management practices and the need to focus on the key strengths of their organisation so that they customise their security management practices accordingly. There is also discussion about the practical implications of this Thesis one which includes the incorporation of the usability characteristics of security tools uncovered in this Thesis through the survey by developers when designing their security tools. There is also reference to the theoretical contributions, including the introduction of the Technological- Organisational–Individual framework. Finally limitations are mentioned, e.g. the survey was conducted with students and not with real employees, since it was not feasible to carry out the survey on such a considerable number of participants, namely 150 employees.

Chapter 10: Conclusions

10.1 Introduction

This Thesis investigates the complex are of security behaviour. In the previous chapters the field of security behaviour was introduced, the challenges in ISP compliance were analysed and the gaps in security behaviour were identified which led to the development of the two research questions. Afterwards, there was description of the research outline and the main body of research was analysed including the usability survey, the development of the Technological-Organisational-Individual framework, the gap analysis of the ISO Standards, the case study and the development of the guidelines. Then findings of the Thesis were analysed, explained and discussed along with the implications for theory and practice.

In this chapter, conclusions of the Thesis are presented. Some of the conclusions include the clarification of literature findings and the development of a comprehensive framework, the investigation of the role of technology in shaping security behaviour and the identification of usability characteristics motivating users to use security and privacy tools, the gap analysis of ISO 27001, 27002, 27003 and 27005 showing that current security management practices are missing important insights with regard to security behaviour and the introduction of a set of practical guidelines to assist security managers when implementing the guidelines provided by the above ISO Standards. As a result this Thesis bridges the gap between theory and practice and facilitates security managers with a handbook they can use to implement security management practices of ISO 27001, 27002, 27003 and 27005 by taking into account the "human aspect" of information security behaviour.

10.2 Overall Conclusions of the Thesis

Although organisations implement security countermeasures to secure their information assets, there are still security breaches attributed to employees because they fail to comply with the ISPs, or use security tools correctly. The employees are often described as the weakest link in the organisation, because the information security of one organisation is only as good as its employees. Although security managers invest in implementing security mechanisms, tools and practices, in the end it is the individual responsible to decide whether to adopt a good security behaviour and protect the organisation from security threats and

breaches or not. To address the human element and identify what factors influence security behaviour an extensive literature review was carried out in order to identify and understand in depth the various security behaviour determinants. The literature review in security behaviour and ISP compliance studies revealed that the role of technology shapes security behaviour but there is limited research. Therefore a usability study was conducted to further investigate which are the usability characteristics that motivate users to use security and privacy tools.

The previous findings led to the development of a Technological-Organisational-Individual Framework that consists of different factors identified through literature and the usability survey groups into categories and written in language that is comprehensible by security managers. This framework consists of a figure that security managers can have as a roadmap and an analysis of the implications of these factors.

Since this Thesis aims to bridge the gap between theory and practice the next step was to analyse in practice current security management practices provisioned in the ISO 27001, 27002, 27003 and 27005 Standards and to conduct a gap analysis based on the factors of the framework. It was found that the human aspect is not adequately addressed and along with other factors, current security management standards do not incorporate the useful insights of the framework.

The Technological-Organisational-Individual framework was then tested for its applicability in a large real life organisation to determine which of the suggested factors are followed in practice and to further bridge the gap between theory and practice. While many of the suggested factors that are stated in the framework are implemented in practice, some shortcomings were identified. Furthermore, recommendations on how to address these shortcomings and on how to further enhance current security management practices were provided.

The final and step of the Thesis was to take all the knowledge gained from the framework, the gap analysis and the case study and produce practical recommendations that security managers can follow to improve their security management practices and supplement their understanding of the guidelines provided by the ISO 27001, 27002, 27003 and 27005. This set of guidelines offer security managers practical information on how to consider the factors of the framework and adopt a comprehensive approach towards security behaviour.

- **Research Question 1: Which factors influence the security behaviour of employees?**

Through the literature review it was identified that current literature findings are not accessible to security managers due to conflicting results (such as the effect of sanctions), different terms being used for similar concepts (such as punishment severity or deterrent severity) and confusing terminology (such as self-efficacy, perceived value congruence) (Topa & Karyda, 2015). This highlighted the difficulties for security managers in grappling with the issue of employees' security behaviour. Many of the studies documented in literature are based on different complex human behavioural theories, such as Theory of Reason Action, Rational Choice Theory, General Deterrence Theory, etc. and lack practical guidance for security managers (Topa & Karyda, 2016). This coupled with the fact that there is no single compilation of all the factors involved in security behaviour leads to a situation where the wealth of information that literature offers is hardly accessible to security managers and may not be of much practical use. Thus, this need for better classification and clarification of the many security behaviour factors was the foundation for the Technological-Organisational-Individual framework which was developed to serve as a roadmap for security managers.

Another finding of the literature review was that while there is reference to the role of technological factors in shaping security behaviour, (Dinev & Hu, 2007), this is limited and narrow in scope (e.g. focusing only on some security factors such as perceived ease of use and perceived usefulness). This led to the more in-depth study of technological factors relevant to usability which impact security behaviour. The review revealed several points for consideration: firstly, there is no single study encompassing all the usability factors, which, as with the general literature review, suggests a lack of accessibility for security managers; secondly, the majority of the characteristics studied are not empirically tested and therefore the significance of these factors is not evidenced; thirdly some factors refer to overlapping concepts such as visibility and feedback, which may create confusion for security managers; and finally, users' views on usability are scarcely addressed. Given the widely held opinion that the human aspect of information security is often overlooked (Bulgurcu et al., 2010), this provided the rationale for a usability survey of security and privacy tools from the user's perspective, which in turn helped to enrich the technological aspects of the framework, including *accessibility, easy and understandable language, intuitiveness (learnability, visibility, locatability, understandability), efficiency, feedback and errors, undo actions, availability of information, design and consistency, availability among platforms, control and*

automisation, characteristics relevant to installation and *privacy characteristics (control of users' data and transparency)* (Topa & Karyda, 2018).

The above findings led to the creation of a Technological-Organisational-Individual framework which provides a way for security managers to understand the complex and multi-faceted nature of security behaviour. This framework suggests that security managers need to adopt a comprehensive approach when designing their security management practices by considering individual characteristics, beliefs, values, by addressing the organisational resources, cultural context, practices and mechanisms and by considering the technical aspects of security tools that make them user-friendly. This framework can be used as a roadmap by security managers when implementing their security management practices. As a result, this framework facilitates security management as it addresses the "human aspect" which is overlooked in security management practices since they have to be generic and address more practical aspects, such as training, sanctions and rewards, etc.

- **Research Question 2: How can the knowledge about these factors be exploited so as to enhance security management practices?**

To answer the second research question an analysis of ISO 27001, 27002, 27003 and 27005 was conducted to identify current security management practices followed by security managers. Then in order to determine which of the factors stated in the literature are addressed in the above security management practice a gap analysis was conducted (Topa & Karyda, 2019). Offering a more comprehensive perspective on security behaviour factors that security managers have to consider when designing and implementing their security management practices, the Technological-Organisational-Individual framework assisted in identifying certain shortcomings of current ISO Standards related to security behaviour. Analysing ISO 27001, 27002, 27003, and 27005, this study identified a number of factors not adequately addressed or incorporated into ISO standards and therefore unlikely to make their way into security management practices, since the majority of organisations base their security practices on guidelines laid down by these standards. Findings of the gap analysis regarding the ISO standards indicate insufficient inclusion of the factors of top management participation, the cultural context, cost of compliance, habits, individual characteristics, perceptions about threats and capabilities, values, different security awareness types, social influence and the different types of usability characteristics (Topa & Karyda, 2019).

To link theory with practice and to test the applicability of the framework a case study was carried out in a large organisation. This led to the conclusion that the Technological-Organisational-Individual framework can be used as a roadmap by security managers. The case study revealed the absence of specific sanctions for ISP non-compliance, the significance attached to the human aspects of information security such as user-friendly ISPs, communication and employee feedback, the promotion of appropriate security behaviour through effective practices, the availability of tools for employees with disabilities and the focus on the development of information security for teleworking. In more general terms, the case study highlights the importance of organisational culture in shaping good employee security behaviour as well as the necessity for organisations to develop security management practices that address the rapidly changing work styles of organisations today.

Another conclusion drawn from the case study is that while organisations need to implement practices recommended by generally accepted standards such as ISO 27001, 27002, 27003 and 27005, a more effective approach may be for organisations to supplement these practices by tailoring their security management practices to suit the needs and the culture of their particular organisation. In other words, to avoid the 'one-size-fits-all' approach and instead exploit the key strengths of their own particular organisational culture. The absence of specified sanctions in the organisation in question are a case in point, as rewarding good security behaviour may be better suited to its organisational culture and values. This justifies the need for a supplementary set of guidelines that security managers can refer to and are included in chapter 8.

Furthermore, another conclusion that emerges from the case study is that organisations need to constantly adjust their security management practices to keep in line with shifting work styles. As traditional workplaces are replaced by more flexible teleworking schemes, employees are using portable devices or their own personal devices when working from home, exposing them to various new security threats and presenting security managers with a new set of challenges to ensure their organisation's security is protected.

One general conclusion of this Thesis is that by considering the factors of the framework, security managers should aim to create an organisational information security culture, since the creation of such a culture will lead employees to enhanced ISP compliance. The case study revealed that the organisation has developed an organisational information security culture through communication, knowledge sharing, mutual support, values and embracing employees' feedback. Moreover, employees are encouraged to comply with ISPs out of habit through the provision of resources and training material that is easily accessible.

This overall security culture motivates employees to comply with ISPs naturally, encouraged by intrinsic motives because they believe that this is the right thing to do.

To achieve the overall aim of this Thesis, namely to enable organisations to exploit the knowledge of the factors influencing security behaviour in practice, enhance security management practices and improve ISP compliance, a set of practical guidelines is developed to be used in conjunction with the Technological-Organisational-Individual framework framework as a handbook for security managers (Topa & Karyda, 2019; Topa & Karyda, 2016). Drawing on all the previous research findings in this Thesis, these clear guidelines bridge the challenging gap between theory and practice, allowing security managers to better understand the full spectrum of factors influencing security behaviour and exploit this information to adopt more effective security management practices, enhance ISP compliance and achieve optimum information security.

Finally, this Thesis provides security managers with the Technological-Organisational-Individual framework and they need to consider all aspects, when designing their security management practices. Security managers by addressing these factors they can have a comprehensive perspective of security behaviour, identify critical points or key strengths in their organisation and design security management practices that best suit their organisation in order to facilitate ISP compliance. Security managers by using this PhD Thesis as a handbook, they can design their security management practices and cultivate an organisational security culture.

The important contribution of this Thesis is that it investigates the area of security behaviour and therefore through the framework security managers are encouraged to look at security management from a different perspective. This perspective focuses on the individual and on the factors that impact his/her security behaviour. Since, security managers are people with technical IT skills and knowledge they are used to implementing security mechanisms and controls to safeguard the information assets of their organisation. However, this Thesis shows them a different angle to implement their practices, which takes into consideration what factors motivate individuals to form a security behaviour. Therefore, it is not just an implementation of security practices but a more demanding intellectual analysis that focuses on the individuals and on what practices are suitable for them. Since technology is developing will continue to develop through the years, security threats will rise in number and complexity. To be able to deal with this situation, security managers need to design security management practices based on factors influencing security behaviour. This is the only way to encourage employees to follow ISPs and use security tools in a technology evolving world. The cultivation of the appropriate security behaviour in an organisation through the creation of a

security culture should be a priority for security managers in the next years as it will motivate employees to comply with ISPs naturally and they will be motivated to protect their organisations from security threats and breaches.

As this Thesis acknowledges, the field of security behaviour is a complex and ever-changing one. As such, there is still a clear need for further research, especially with regard to factors influencing users to follow ISPs when teleworking or when they use their own devices, the effect of sanctions and rewards and the role of organisational and cultural context with regard to security behaviour. Another area for research is the creation of guidelines for developers on how to design and implement usable security tools as well as integrating the usability characteristics that were identified in this Thesis to design and implement usable security and privacy tools.

Research Questions	Conclusions	Publications
1. Which factors influence the security behaviour of employees?	• Literature findings about security behaviour are not accessible to security managers, due to confusing terminology, conflicting results, similar concepts are introduced under different names, inadequate guidance of the implications of factors in practice. • The role of technology and of the usability characteristics from the users' perspective while important is not adequately addressed in literature studies of IS. • Usability characteristics such as *accessibility, easy and understandable language, intuitiveness (learnability, visibility, locatability, understandability), efficiency, feedback and errors, undo actions,*	(Topa & Karyda, 2015), (Topa & Karyda, 2016), (Topa & Karyda, 2018)

	availability of information, design and consistency, availability among platforms, control and automation, characteristics relevant to installation and privacy characteristics (control of users' data and transparency) Were found as important by users. • Development of a Technological-Organisational-Individual Framework, which can be employed as a roadmap for security managers when implementing their security management practices	
2. How can the knowledge about these factors be exploited so as to enhance security management practices?	• Security management practices of ISO Standards 27001, 27002, 27003 and 27005 lack important insights of the Technological-Organisational-Individual framework with regard to ISP compliance. These standards do not adequately cover or do not cover at all factors included in the framework such as *top management participation, the cultural context, cost of compliance, habits, individual characteristics, perceptions about threats and capabilities, values, different security awareness types, social influence and the different types of usability characteristics.* • The case study validates the applicability of the Technological-	(Topa & Karyda, 2019) (Topa & Karyda, to be submitted)

	Organisational-Individual framework. It was found that while the majority of the practices are effective, some shortcomings were identified, and recommendations were given, such as implementation of a rewarding mechanism for employees who identify a malicious phishing email, informing employees about the role of the LISO, suggesting that sanctions might not be an effective practice for this organisation, etc. • Security managers by addressing the factors of the Technological-Organisational-Individual framework they can have a comprehensive perspective of security behaviour, identify critical points or key strengths in their organisation and design security management practices that best suit their organisation in order to facilitate ISP compliance. • This Thesis through the Technological-Organisational-individual framework and the set of guidelines can act as a handbook for security managers when implementing their security management practices.	

Table 6: Conclusions and Findings of the Thesis

References

Andriotis, P., Oikonomou, G., Mylonas, A., & Tryfonas, T. (2016). A study on usability and security features of the android pattern lock screen. Information & Computer Security, 24(1), 53-72.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), pp. 523-548.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. Computer Fraud & Security, 2010(3), 13-19.

Clark, J., Van Oorschot, P. C., & Adams, C. (2007, July). Usability of anonymous web browsing: an examination of tor interfaces and deployability. In Proceedings of the 3rd symposium on Usable privacy and security (pp. 41-51). ACM.

COBIT. (2007). COBIT 4.1. IT Governance Institute.

Coles-Kemp, L., & Theoharidou, M. (2010). Insider threat and information security management. In Insider threats in cyber security. Springer US, pp. 45-71.

Collett,S.(2015). Five sneaky ways companies are changing employees' security behavior. CSOonline. Available at: https://www.csoonline.com/article/2881940/security-awareness/five-sneaky-ways-companies-are-changing-employees-security-behavior.html (Accessed 10 Jan. 2018)

Connolly, L., Lang, M., & Tygar, J. D. (2015). Investigation of Employee Security Behaviour: A Grounded Theory Approach. In ICT Systems Security and Privacy Protection. Springer International Publishing, pp. 283-296.

Cranor, L. F., & Buchler, N. (2014). Better together: Usability and security go hand in hand. IEEE Security & Privacy, 12(6), 89-93.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, pp. 90-101.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security, 22(5), pp. 474-489.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), pp. 79-98.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organisations. Information Systems Journal, 16(3), pp. 293-314.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. Computers in Human Behavior, 61.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information Systems, 8(7), p. 386.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. Information Systems Journal, 19(4), pp. 391-412.

Enisa report (2016). PETs controls matrix A systematic approach for assessing online and mobile privacy tools (2016)

EY Global Information Security Survey (2019). Is Cybersecurity about more than protection? EY, 2019, available at: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf (accessed 6 July 2019)

Flechais, I., Mascolo, C., & Sasse, M. A. (2007). Integrating security and usability into the requirements and design process. International Journal of Electronic Security and Digital Forensics, 1(1), 12-26.

Furnell, S.(2010). Usability versus complexity-striking the balance in end-user security, Network Security, 13–17

Furnell, S. (2016). The usability of security–revisited. Computer Fraud & Security, 2016(9), 5-11.

Garza, V., & Guo, X. (2015). Securing BYOD: A study of framing and neutralization effects on mobile device security policy compliance.

Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), pp. 106-125.

Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organisations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), pp. 154-165.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Information Systems Journal, 24(1), pp. 61-84.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organisational culture. Decision Sciences, 43(4), pp. 615-660.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), pp. 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69-79.

ISO 27001. (2013). ISO/IEC 27001:2013. Information technology-Security techniques-Information security management systems-Requirements.

ISO 27002. (2013). ISO/IEC 27002:2013. Information technology-Security techniques-Code of practice for information security controls.

ISO 27003. (2010). ISO/IEC 27003:2010. Information technology-Security techniques-Information security management system implementation guidance.

ISO 27005. (2011). ISO/IEC 27005:2011. Information technology-Security techniques-Information security risk management.

ISO 9241-11. (1998). ISO 9241-11:1998 Ergonomic requirements for office work with visual display terminals (VDTs) Part 11: Guidance on usability

ISO Survey. (2017). ISO Survey for 2017. Available at: https://www.iso27001security.com/html/27001.html (accessed 6 July 2019)

IT Governance Institute. (2008). Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit.

Johnston, J., Eloff, J. H., & Labuschagne, L. (2003). Security and human computer interfaces, 2003. Comput. Secur. 22, 675–684. https://doi.org/10.1016/S0167-4048(03)00006-3

Karyda, M. (2017). Fostering Information Security Culture In Organisations: A Research Agenda. MCIS

Karyda, M., & Mitrou, L. (2016). Data Breach Notification: Issues and Challenges for Security Management. In MCIS (p. 60).

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), pp. 246-260.

Kaspersky report (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Kaspersky daily, available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (accessed 6 July 2019)

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). Shadow security as a tool for the learning organisation. ACM SIGCAS Computers and Society, 45(1), pp. 29-37.

Kolkowska, E. (2011). Security subcultures in an organisation-exploring value conflicts. In ECIS.

Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking.

Krol, K., Spring, J. M., Parkin, S., & Sasse, M. A. (2016). Towards robust experimental design for user studies in security and privacy. In The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016) (pp. 21-31).

Lambrinoudakis, C. (2013). Evaluating and enriching information and communication technologies compliance frameworks with regard to privacy. Information Management & Computer Security, 21(3), pp. 177-190.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review, 37(12), pp. 1049-1092.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM, 48(8), 72-77.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal, 25(5), pp. 433-463.

Maykut, P. & Morehouse, R.(1994). Beginning Qualitative Research: A Philosophic and Practical Guide. The Falmer Press, London.

Mitrou, L. (2017a). The General Data Protection Regulation. New Regulation – New Responsibilities-New rights, 1st edition, Sakkoula Publishing

Mitrou, L. (2017b). The General Data Protection Regulation: A Law for the Digital Age?. In EU Internet Law (pp. 19-57). Springer, Cham.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. MIS Quarterly, 42(1).

Murayama, Y., Fujihara, Y., Saito, Y., & Nishioka, D. (2012). Usability issues in security. In International Workshop on Security Protocols (pp. 161-171). Springer, Berlin, Heidelberg.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules; an empirical study. European Journal of Information Systems, 18(2), pp. 126-139.

Năstase, P., Năstase, F., & Ionescu, C. (2009). Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. Economic Computation & Economic Cybernetics Studies & Research, 43(3), pp. 5-20.

Nielsen J. (2005). 10 Usability Heuristics for User Interface Design. [online] Available at: https://www.nngroup.com/articles/ten-usability-heuristics/

Nielsen, J. (1994). Usability engineering. Elsevier

Pahnila, S., Karjalainen, M., & Siponen, M. T. (2013). Information Security Behavior: Towards Multi-Stage Models. In PACIS. p. 102.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In 40th Hawaii International Conference on System Sciences HICSS 2007. IEEE, pp. 156b-156b.

Payne, B. D., & Edwards, W. K. (2008). A brief introduction to usable security. IEEE Internet Computing, 12(3), pp.13-21.

RedTeam (2018). Dangers In Your Ranks: 7 Times Employees Caused Damaging Data Breaches. Available at: https://www.redteamsecure.com/danger-ranks-7-times-employees-caused-data-breaches/ (accessed 6 July 2019)

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in Organisations. Computers & Security, 56, pp. 70-82.

Schein, E. H. (2010). Organizational culture and leadership (Vol. 2). John Wiley & Sons.

Seffah, A., Donyaee, M., Kline, R. B., & Padda, H. K. (2006). Usability measurement and metrics: A consolidated model. Software Quality Journal, 14(2), 159-178.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, pp. 177-191.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), pp. 267-270.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), pp. 217-224.

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. In Innovations in Information Technology, IEEE, pp. 1-5.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies. Information Management & Computer Security, 22(1), pp. 42-75.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management, 48(7), pp. 296-302.

Spyridopoulos, T., Topa, I. A., Tryfonas, T., & Karyda, M. (2014, June). A holistic approach for cyber assurance of critical infrastructure with the viable system model. In IFIP International Information Security Conference (pp. 438-445). Springer, Berlin, Heidelberg.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. Risk management guide for information technology systems.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences (IJECSIJENS), 11(5), pp. 23-29.

Symantec (2017). Symantec Security Response Team. Symantec Blogs. Petya ransomware outbreak: Here's what you need to know. Accessed online at: https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper

Techcrunch. (2019). Two years after WannaCry, a million computers remain at risk. Accessed online at: https://techcrunch.com/2019/05/12/wannacry-two-years-on/

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6), 472-484.

Thomson, K. L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. Computer fraud & security, 2006(10), 7-11.

Topa, I, & Karyda, M., (2016). Analyzing security behaviour determinats for enhancing ISP compliance and security management. In European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS).

Topa, I. & Karyda, M., (2018). Usability of Security and Privacy Tools: The Users' Perspective. IFIP SEC 2018

Topa, I., & Karyda, M. (2015). Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In Trust, Privacy and Security in Digital Business. Springer International Publishing, pp. 169-179.

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. Information & Computer Security.

Topa, I. & Karyda M. (to be submitted). Addressing Organisational, Individual and Technological Aspects in Information Security Management (to be submitted)

Tsohou, A., Karyda, M., & Kokolakis, S. (2015a). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers & security, 52, 128-141.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015b). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38-58.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2009). Information systems security management: a review and a classification of the ISO standards. In International Conference on e-Democracy (pp. 220-235). Springer, Berlin, Heidelberg.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. Information Management & Computer Security, 18(5), 350-365.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management, 49(3), pp. 190-198.

Vemou, K., Mousa, G., and Karyda, M., (2015). On The Low Diffusion Of Privacy Enhancing Technologies In Social Networking: Results Of An Empirical Investigation.EMCIS 2015

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. Decision Support Systems.

Wästlund, E., Fischer Hübner, S., Graf, C., Hochleitner, C., Wolkerstorfer, P., Angulo, J., 2011. Towards Usable Privacy Enhancing Technologies : Lessons Learned from the PrimeLife Project. PrimeLife.

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security, 28(1), 47-62.

Western Sydney University. (2016). Case study structure. Assessed online at: https://www.westernsydney.edu.au/__data/assets/pdf_file/0008/1082474/Case_Study_Structure.pdf

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In USENIX Security Symposium (Vol. 348).

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS quarterly, 37(1), pp.1-20.

Yee, K. P. (2004). Aligning security and usability. IEEE Security & Privacy, 2(5), 48-55.

Yin, R. K. (2011). Applications of case study research. sage.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), pp. 330-340.

Annex A

1. Description of the Scenarios

1.1 Scenario 1:

1. Open Google Chrome or Firefox. Deactivate if you have extensions for Ad-blocking
2. Open the link https://www.ghostery.com/3. Download and install the English version of Ghostery and create an account and register with your personal data
4. Use the browser to open the link: https://store.playstation.com/#!en-gr/home/games
5. In this website restrict all trackers relevant to advertisement
6. Open the link https://security.stackexchange.com/questions
7. Block google analytics
8. Set the purple box to always appear in the right corner of the website.
9. Open the link http://www.nvidia.com/Download/index.aspx?lang=en-us
10. Block the trackers form Site Analytics and restrict the trackers for social media.
11. Open the link: https://www.wired.com/category/security/
12. Block all trackers
13. Open the link: https://www.wired.com/category/security/
14. Block slow or non-secure trackers
15. Open the link: https://www.coursera.org/
16. Restrict this website
17. Change the settings so that the tool can block every new tracker by default
18. Undo all trackers that were previously blocked
19. Undo al trackers that were previously restricted.

1.2 Scenario 2:

1. Open a browser
2. Open the link https://www.malwarebytes.com/premium/
3. Download and install the English version of Malwarebytes
4. Select the option “scan for rootkits” from the settings
5. Carry out a threat scan

6. Delete any malware that was identified
7. Review the report that appears after the scan
8. Carry out a custom scan
9. Select all the available disks and “scan for rootkits”;
10. Delete any malware that was identified
11. Review the report that appears after the scan

1.3 Scenario 3:

1. Open a browser
2. Open the link https://www.torproject.org/download/download
3. Download and install the English version of Tor
4. Test the security settings of Tor
5. Use the appropriate search engine
6. Check that https everywhere is enabled
7. Check that block pop-up windows is enabled
8. Change security settings so that history is never saved
9. Set security level to high;
10. Open the link: https://www.playstation.com/en-us/explore/games/newreleases/
11. Change the settings to view its content (by minimising the security level and temporarily allowing the scripts);
12. Maximise security level and revoke the permissions;
13. Open the link: https://www.wired.com/category/security/
14. In order to view the contents of the website that are not available deactivate the scripts globally
15. Undo the restriction of the scripts globally
16. Open the link: https://my-samos.blogspot.gr/
17. Check whether your connection is secure
18. Maximise the window
19. Before closing the browser create a New Identity

2. Questionnaires

2.1 Questionnaire for the use of Ghostery

1. Installation process

1. How did you find the installation process?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

2. How important is it for you that the installation process is easy?

- Very important
- Important
- Neutral
- Little important
- Unimportant

3. How important is it for you that you avoid revealing your personal data for ease of use of the installation process?

- Very important
- Important
- Neutral
- Little important
- Unimportant

4. Were there the minimum requirements for the installation, e.g. specific operational system of the tool clearly stated?

    - Yes
    - No

5. How did you find the changes that took place on the browser after installation?

- Very positive
- Positive
- Neutral
- Negative
- Very negative

2.Use of the tool

6. Describe briefly which is the scope of the tool?

2.1 Available information and support

7. If you used any form of available information or support to learn how to use the tool, which of the following was it?
    - Live demos/video
    - FAQs
    - Quick Tour
    - Email address
    - Other, please describe:

8. If you made use of any of the previous forms of support, were they adequate?
    - Yes
    - No

9. If no, in which case was there no support?

10. How important is it for you that you have access to available information or support?
    - Very important
    - Important
    - Neutral
    - Little important
    - Unimportant

2.2 Language

11. Was language easy to understand?

- Yes
- No

12. Were you able to tell the difference between “block” and “restrict”?

- Yes
- No

13. If yes, explain the difference.

14. How important is it for you that the language does not have many technical terms?

- Very important
- Important
- Neutral
- Little important
- Unimportant

2.3 Design and feedback

15. How easy was it to find what you were looking for?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

16. If it was difficult, please describe

17. How important is it for you to find what you were looking for easily?

- Very important
- Important
- Neutral
- Little important

- Unimportant

18. Did you always know what to do next (which was he next step)?
- Yes
- No

19. Were there cases when you did not know what to do next? Please describe

20. How important is it for you that you always know what to do next?
- Very important
- Important
- Neutral
- Little important
- Unimportant

21. While you were carrying out the tasks, did you receive any feedback (e.g. notifications, messages, information) from the tool?
- Yes
- No

22. Was it visible?
- Yes
- No

23. If no, what would attract your attention?

24. How important is it for you that you receive feedback?
- Very important
- Important
- Neutral
- Little important
- Unimportant

25. Were there status indicators (e.g. figures or pictures) showing you of your privacy is protected (e.g. if the trackers were blocked) and in what degree?

- Yes
- No

26. If yes, which status indicators did you notice?

27. If yes, how important is it for you that there are status indicators to show you if your privacy is protected and in what degree?

- Very important
- Important
- Neutral
- Little important
- Unimportant

28. Did the tool inform you if you made any errors?

- Yes
- No

29. If yes, did the tool inform you how to prevent the error?

- Yes
- No

30. How important is it for you to be informed about the errors that you make?

- Very important
- Important
- Neutral
- Little important
- Unimportant

31. Did you undo some actions during the process?

- Yes
- No

32. If yes, please describe.

33. How important is it for you to be able to undo your actions?

- Very important
- Important
- Neutral
- Little important
- Unimportant

34. Were there advanced settings?

- Yes
- No

35. How important is it for you that there are advanced settings?

- Very important
- Important
- Neutral
- Little important
- Unimportant

2.4 Privacy settings

36. Were you able to change the privacy settings?

- Yes
- No

37. If yes, please describe what changes did you make

38. How important is it for you to change the privacy settings?

- Very important
- Important
- Neutral
- Little important
- Unimportant

3 Overall assessment

39. How effective so you think the tool is?

- Very effective
- Effective
- Neutral
- Little effective
- Ineffective

40. How easy is it for you to learn how to use the tool?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

42. How satisfied are you from using the tool?

- Very satisfied
- Satisfied
- Neutral
- Little satisfied
- Not satisfied

43. Please state which aspects you liked the most

- Easy installation
- Available information and support
- Minimalistic design
- Status indicators to show if my privacy is protected
- To find what I am looking for easily
- Adequate protection of privacy
- Ease of learning how to use the tool

44. Please describe if there were any problems during using the use of the tool.

45. Will you install the tool in your computer?

- Yes
- No

46. If not, please select the reason

- Inappropriate minimum installation requirements
- I am not interested in privacy
- I do not like the use of this tool
- Browsing on the internet is done with difficulties
- It is time consuming
- Other, please describe:

2.2 Questionnaire for the use of Malwarebytes

1. Installation process

1. How did you find the installation process?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

2. How important is it for you that the installation process is easy?

- Very important
- Important
- Neutral
- Little important
- Unimportant

3. How important is it for you that you avoid revealing your personal data for ease of use of the installation process?

- Very important
- Important
- Neutral
- Little important
- Unimportant

4. Were there the minimum requirements for the installation, e.g. specific operational system of the tool clearly stated?
    - Yes
    - No

5. How did you find the changes that took place on your computer after installation?
    - Very positive
    - Positive
    - Neutral
    - Negative
    - Very negative

2.Use of the tool

6. Describe briefly which is the scope of the tool?

2.1 Available information and support

7. If you used any form of available information or support to learn how to use the tool, which of the following was it?
    - Live demos/video
    - FAQs
    - Forum
    - Manual
    - Other, please describe:

8. If you made use of any of the previous forms of support, were they adequate?
    - Yes
    - No

9. If no, in which case was there no support?

10. How important is it for you that you have access to available information or support?
    - Very important
    - Important
    - Neutral
    - Little important
    - Unimportant

2.2 Language

11. Was language easy to understand?
- Yes
- No

12. Were you able to tell the difference between “threat scan” and “custom scan”?
- Yes
- No

13. If yes, explain the difference.

14. How important is it for you that the language does not have many technical terms?
- Very important
- Important
- Neutral
- Little important
- Unimportant

2.3 Design and feedback

15. How easy was it to find what you were looking for?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

16. If it was difficult, please describe

17. How important is it for you to find what you were looking for easily?

- Very important
- Important
- Neutral
- Little important
- Unimportant

18. Did you always know what to do next (which was he next step)?

- Yes
- No

19. Were there cases when you did not know what to do next? Please describe

20. How important is it for you that you always know what to do next?

- Very important
- Important
- Neutral
- Little important
- Unimportant

21. While you were carrying out the tasks, did you receive any feedback (e.g. notifications, messages, information) from the tool?

- Yes
- No

22. Was it visible?

- Yes
- No

23. If no, what would attract your attention?

24. How important is it for you that you receive feedback?

- Very important
- Important
- Neutral
- Little important
- Unimportant

25. Were there status indicators (e.g. figures or pictures) showing you if your security is protected and in what degree?

- Yes
- No

26. If yes, which status indicators did you notice?

27. If yes, how important is it for you that there are status indicators to show you if your privacy is protected and in what degree?

- Very important
- Important
- Neutral
- Little important
- Unimportant

28. Did the tool inform you if you made any errors?

- Yes
- No

29. If yes, did the tool inform you how to prevent the error?

- Yes

- No

30. How important is it for you to be informed about the errors that you make?
- Very important
- Important
- Neutral
- Little important
- Unimportant

31. Did you undo some actions during the process?
- Yes
- No

32. If yes, please describe.

33. How important is it for you to be able to undo your actions?
- Very important
- Important
- Neutral
- Little important
- Unimportant

34. Were there advanced settings?
- Yes
- No

35. How important is it for you that there are advanced settings?
- Very important
- Important
- Neutral
- Little important
- Unimportant

2.4 Security settings

36. Were you able to change the security settings?

- Yes
- No

37. If yes, please describe what changes did you make

38. How important is it for you to change the security settings?

- Very important
- Important
- Neutral
- Little important
- Unimportant

3 Overall assessment

39. How effective so you think the tool is?

- Very effective
- Effective
- Neutral
- Little effective
- Ineffective

40. How easy is it for you to learn how to use the tool?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

42. How satisfied are you from using the tool?

- Very satisfied
- Satisfied

- Neutral
- Little satisfied
- Not satisfied

43. Please state which aspects you liked the most

- Easy installation
- Available information and support
- Minimalistic design
- Status indicators to show if I am protected in terms of security
- To find what I am looking for easily
- Adequate protection of security
- Ease of learning how to use the tool
- Other, please describe:

44. Please describe if there were any problems during using the use of the tool.

45. Will you install the tool in your computer?

- Yes
- No

46. If not, please select the reason

- Inappropriate minimum installation requirements
- I am not interested in security
- I do not like the use of this tool
- My computer is not efficient
- It is time consuming
- Other, please describe:

2.3 Questionnaire for the use of Tor

1. Installation process
    1. How did you find the installation process?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

2. How important is it for you that the installation process is easy?

- Very important
- Important
- Neutral
- Little important
- Unimportant

3. How important is it for you that you avoid revealing your personal data for ease of use of the installation process?

- Very important
- Important
- Neutral
- Little important
- Unimportant

4. Were there the minimum requirements for the installation, e.g. specific operational system of the tool clearly stated?
    - Yes
    - No

5. How did you find the changes that took place on the computer after installation?
    - Very positive
    - Positive
    - Neutral
    - Negative
    - Very negative

2.Use of the tool

6. Describe briefly which is the scope of the tool?

2.1 Available information and support

7. If you used any form of available information or support to learn how to use the tool, which of the following was it?
    - FAQs
    - Forum
    - Manual
    - Other, please describe:

8. If you made use of any of the previous forms of support, were they adequate?
    - Yes
    - No

9. If no, in which case was there no support?

10. How important is it for you that you have access to available information or support?
    - Very important
    - Important
    - Neutral
    - Little important
    - Unimportant

2.2 Language

11. Was language easy to understand?
- Yes
- No

12. Were you able to tell the difference between “temporarily allow all in this page” and “allow scripts globally”?

- Yes
- No

13. If yes, explain the difference.

14. How important is it for you that the language does not have many technical terms?
- Very important
- Important
- Neutral
- Little important
- Unimportant

2.3 Design and feedback

15. How easy was it to find what you were looking for?
- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

41. If it was difficult, please describe

42. How important is it for you to find what you were looking for easily?
- Very important
- Important
- Neutral
- Little important
- Unimportant

43. Did you always know what to do next (which was he next step)?
- Yes
- No

44. Were there cases when you did not know what to do next? Please describe

45. How important is it for you that you always know what to do next?

- Very important
- Important
- Neutral
- Little important
- Unimportant

46. While you were carrying out the tasks, did you receive any feedback (e.g. notifications, messages, information) from the tool?

- Yes
- No

47. Was it visible?

- Yes
- No

48. If no, what would attract your attention?

49. How important is it for you that you receive feedback?

- Very important
- Important
- Neutral
- Little important
- Unimportant

50. Were there status indicators (e.g. figures or pictures) showing you of your privacy is protected (e.g. if the scripts are blocked) and in what degree?

- Yes
- No

51. If yes, which status indicators did you notice?

52. If yes, how important is it for you that there are status indicators to show you if your privacy is protected and in what degree?

- Very important
- Important
- Neutral
- Little important
- Unimportant

53. Did the tool inform you if you made any errors?

- Yes
- No

54. If yes, did the tool inform you how to prevent the error?

- Yes
- No

55. How important is it for you to be informed about the errors that you make?

- Very important
- Important
- Neutral
- Little important
- Unimportant

56. Did you undo some actions during the process?

- Yes
- No

57. If yes, please describe.

58. How important is it for you to be able to undo your actions?

- Very important
- Important
- Neutral
- Little important

- Unimportant

59. Were there advanced settings?

- Yes
- No

60. How important is it for you that there are advanced settings?

- Very important
- Important
- Neutral
- Little important
- Unimportant

2.4 Privacy settings

61. Were you able to change the privacy settings?

- Yes
- No

62. If yes, please describe what changes did you make.

63. How important is it for you to change the privacy settings?

- Very important
- Important
- Neutral
- Little important
- Unimportant

3 Overall assessment

64. How effective so you think the tool is?

    - Very effective
    - Effective

- Neutral
- Little effective
- Ineffective

65. How easy is it for you to learn how to use the tool?

- Very easy
- Easy
- Neutral
- Difficult
- Very difficult

42. How satisfied are you from using the tool?

- Very satisfied
- Satisfied
- Neutral
- Little satisfied
- Not satisfied

43. Please state which aspects you liked the most

- Easy installation
- Available information and support
- Minimalistic design
- Status indicators to show if my privacy is protected
- To find what I am looking for easily
- Adequate protection of privacy
- Ease of learning how to use the tool

44. Please describe if there were any problems during using the use of the tool.

45. Will you install the tool in your computer?

- Yes
- No

46. If not, please select the reason

- Inappropriate minimum installation requirements
- I am not interested in privacy
- I do not like the use of this tool
- Browsing on the internet is done with difficulties
- It is time consuming
- Other, please describe:

3. Interview Questions

1. Which are the positive and which are the negative aspects of the tools?
2. Are you using other similar tools? If yes, which one you prefer and for what reason?
3. How much time did it take you to find the tasks you had to carry out?
4. If you were to redesign the tool which aspects would you keep and which aspects would you change? What changes would you suggest for improving the tool?
5. If you were to improve usability, what changes would you made?
6. Do you intend to use this tool in the future, yes or no and why?