UNIVERSITY OF AEGEAN

SCHOOL OF ENGINEERING

DEPARTMENT OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

MSc in Information and Communication Systems Security

Information Systems Security Management

Evaluating Employees
Information Security Awareness Case Study

MSc Thesis

Alexandra Koutsiafti

Thesis supervisors: Professor Karyda Maria

Examination Board Members: Mr. S. Kokolakis, Mrs L. Mitrou

Samos, January 2020

Contents

1. Acknowledgement

Starting, i would like to thank professor Karyda Maria for supervising this research, for her advices throughout this project and her assistance with guideline.

I also, want to thank my CEO Elly Yannoukaki who provide me the area of exploration in "real working world" and to made me realize how things work in practice.

Finally, I thank my wonderful family (my husband and my parents) for all their support and patience during MSc.

This paper is dedicated to my 5 ½ years old son, who's personal hours have been "stolen" in order my goals to be achieved – to deliver a real and accurate exercise.

2. Abstract

For many years now information security programs are more focused in technical solution i.e. intrusion detection systems, firewalls, anti-virus programs etc, than in human element. Researchers and experts in the information security field state that the user is the weakest link in the chain when it comes to information security. The human error is still the key concept that might threaten information of the organization. Thus, the challenge for many companies, organizations or institutions is to develop a user information Security Awareness Culture.

Based on ENISA, the concept of Cybersecurity Culture refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies. CSC encompasses familiar topics including cybersecurity awareness and information security frameworks but is broader in both scope and application, being concerned with making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions [11].

It is high important to identify the Information Security Awareness program that best improves the user's knowledge and behaviour towards information security. To ascertain the effectiveness of an awareness program, it is essential to assess it.

In this thesis a survey is realized in "real working world" in order to examine the effectiveness of the information security awareness program. In this working area, information security awareness Program is realized annually - mandatory presence for all employees - as this is a requirement for ISO 27001:2013 certification. The design of security awareness Program is descripted in detailed in this writing.

The results from the statistical analysis of the data form the survey have shown that the Awareness Program used in this case were effective. Summarizing the overall results, the survey pointed out that the Effectiveness of the Awareness Program is satisfactory reaching the 91%, rising the Rating Maturity scale to "High", meaning that Employees are aware of good security principles and threats, have been properly trained and comply with company's security and policies. As expected, this result is fully satisfactoriness. This Overall result it holds a strong "Value" due to of the massive participation of employees 96% (31 of 33 employees participate in Awareness Program and Survey). Based on that it is strongly believed that management support enforces the employees into a massive participation, since none of the training method would work without participants.

On the other hand, based on data analysis, there are some areas that need attention as they effect Objective number 3 and both Evaluation Categories. It is clearly understood that based on the failure responds on these 4 questions, it is needed to enforce stronger Awareness on Password

Management and Social engineering, maybe to re-adjust the Awareness Program method from "Web based" to other methods such as classroom or either to extent the Program with Posters, Screensavers, News Letters.

3. The Need for Security Awareness

The latest 2019 Symantec Internet Security Threat Report [6] presents that users are the most at risk of falling victim to email-based malware with Office files, for 48% of malicious email attachments, jumping from 5% in 2017. They also present that spam levels continued to increase in 2018, as they have done every year since 2015, with 55 percent of emails received in 2018 being categorized as spam. In addition, "Verizon 2019 Data Breach Investigations Report" [7] presents that 94% of breaches recorded was through email using Microsoft Office files for 45%. Since they have established a bit of a problem with malicious emails, they wanted to dig more into the user security awareness. *Figure 1* below, "Verizon 2019 Data Breach Investigations Report" [7], shows how quickly employees are clicking or reporting on phishing emails. Users are clicking and reporting, but reporting drops off after the first hour. Users are not aware of the importance of the information security, or they may not have a clear understanding about the risk.

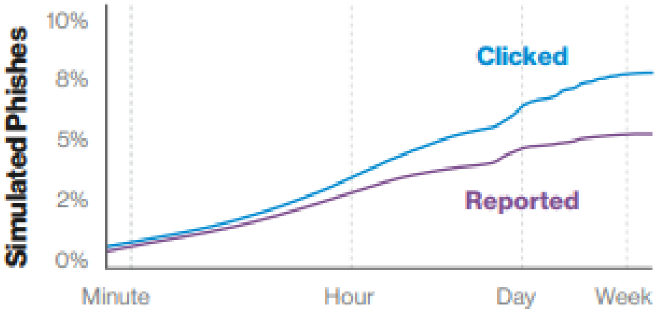


Figure 1: Click and responding rate in public simulated phishes over time

Several international standards and Frameworks refer to Security Awareness as a prerequisite such as ISO 27001:2013 [1], COBIT, CIS [2] and PCI DSS [3]. Furthermore, several campaigns have been organized such as "European Cyber Security Month, 2017" [4] and "SANS, 2019 Security Awareness Report" [5] that includes Information Security Awareness.

This indication highlights the importance of information security awareness and explains the indication of being prerequisite for complying with the standards.

Information security awareness Program is necessary as described form "ENISA Information Security awareness guide" [7] in deferent factors (Internal or External) such as:

- To face new risk / security incidents.
- To comply with new Regulations / Laws / Standards or best practices.
- To address the organization Security Policy / Strategy.
- To Jump on from security awareness to security culture.
- To fullfield Certification requirements.

Last but not least, "EY Global Information Security Survey 2018–19" [8] refers to the need to invest on Information Security Awareness in order to be protected and optimize information security.

"Build awareness around phishing and malware, become 'click-smart"

4. Case Study

4.1. Company

This paper explores Information Security Awareness at a real working environment. The Company established in 1992. During these years the Company is considered as a strategic ICT/OT security and GRC Services partner (Governance, Risk and Compliance), trusted by numerous organizations of different sizes and footprint across 4 continents. Company's portfolio includes only successful projects and happy customers in developing Security Systems, performing IT/OT Audits and participating in Compliance audit teams under GDPR, SOX, PCI DSS, ISO27001, in many industries such as: Large Business Advisor in Assurance/Audit/Tax, International ferry services, Aluminium suppliers, Energy providers, Shipping cargo/trading, independent asset management, private and institutional investors, Medical disposable products, Hospital facilities, Health Insurance, Non-governmental organizations, Banking, Law firms, SW Platform Technologies consulting services, Advertising services, Bakery concept group of stores, Retailing products etc.

The Company invest in its team to ensure a high standards services delivery to customers and to comply with regulations such as GDPR and regular agreements with customers such as NDA's. To achieve its goals, the Company hold ISO27001 certification for its Customer services and implements an Information Security Management System with components, its Organization and Security Awareness.

4.2.Organization

Within this context, IS Steering Committee is created. The IS Steering Committee consists of the Chief Executive Officer, the Service Delivery Manager and the IT Manager. The Chief Information Security Officer participates as a «Rapporteur». The main responsibilities of the IS Steering Committee are:

- To align the information technology strategy with the Company's strategy.
- To define the content of Policies, Procedures and Forms that are part of ISMS.
- To Approve Policies, Procedures and Forms that are part of ISMS.
- Approve budget regarding information security.
- To enforce information security policies.
- To promote security awareness.
- To receive reports (or audit findings) from the Information Security Officer (or an appointed 3rd party IT auditor) and to act accordingly.
- To accept the IT Risk Treatment Plan, thus accepting the Risk exposure, derived from the Risk Assessment process of the CISO.

The Chief Information Security Officer accepts primary responsibility for the development and implementation of information security programs of the Company. His/ Her responsibilities include the following:

- Supervise and monitor the implementation of the information security policy and associated procedures and security measures applicable to the Company.
- Periodically evaluate (by performing audits) the application of the ISMS and identify any needs for changes / adjustments necessary.

- Develop plans, budget and status reports and any other reports required by management committee regarding information security.
- Review of major security breaches and help in developing protective strategies to prevent their reoccurrence.
- Report to the IS Steering Committee the information security incidents
- Be the contact person with external auditors and regulatory representatives regarding information security.
- Prepare the information security risk assessment program and risk treatment plan.
- Co-ordination of education, information and awareness of employees regarding information security issues each year at the first quarter.
- Periodically perform reviews to ensure compliance with the Company's ISMS and associated procedures.
- Prepare and maintain the Statement of Applicability.
- Maintain registry of the Assets of the Company.
- Assess, in collaboration with the Service Delivery Office, the severity of information security incidents.
- Supervise the collection of evidence regarding serious information security incidents.
- Assess the risks involved in change management procedure.
- Provide annual report on incidents to the IS Steering Committee, or exceptionally, in case of an abnormal number or type of incidents.
- Annually sent to Department Managers, the access rights of their personnel, to be approved.
- Review and Approve Change request regarding security issues.

The basic responsibilities of the Service Delivery Manager regarding the Information Security context are documented as follows:

- To ensure confidentiality, integrity and availability, of the Company's and the client data during operations.
- To comply to the Information Security Management System (ISMS), that will contain the appropriate policies and procedures that will define how the Company protects its information from the relative risks.
- To specify the user access rights to information systems, according to the Policy requirements.
- Cooperate with the Chief Information Security Officer or appointed Auditors, for the regularly audits, reporting, or security incident issues.

The IT Manager performs as the link between the Management of the Company and the Service Delivery Office. More specifically, the IT Manager is responsible for the following:

- The project management and the coordination of the implementation of all IT related projects.
- The monitoring of the evolution and current trends of latest technologies and the proposal to the Management, the adaptation of these new technologies for the benefit of achieving the desirable business goals.
- Coordinate and interact for the effectiveness of Help Desk internal support.
- The effectiveness of the backup Policy of the company.
- The effectiveness of the Information Security, taking care of upgrading the systems, applications and configuration to prevent systems from most known threats and to reduce the risks arising from them

Departmental Managers are assigned the responsibility to manage the Company's information resources. Department's managers must be designated as the owners of information used for regular business activities. The responsibilities of the business owners are:

- Specify access control requirements and make periodic reviews of the users' access rights to information assets.
- Cooperate with the Chief Information Security Officer for the Risk Assessment.

The following *Figure 2* displays the organizational structure.

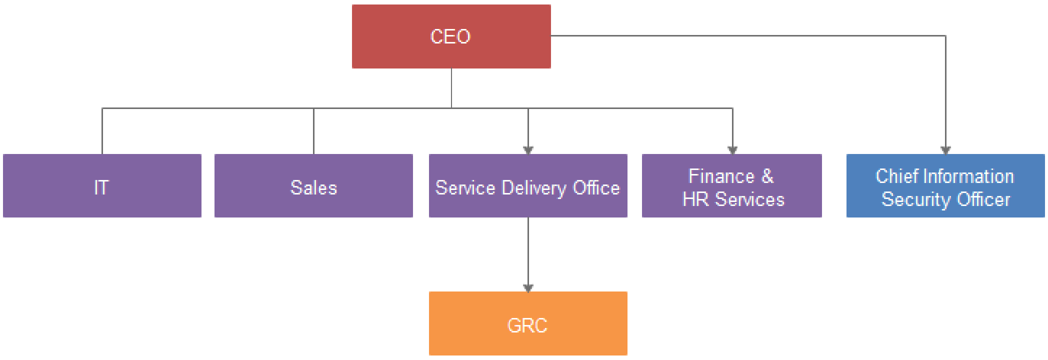


Figure 2: Company's organizational structure

4.3.Security Awareness Program

In this working area, information security awareness Program is realized annually - mandatory presence for all employees - as this is a requirement for ISO 27001:2013 certification. The design of security awareness Program is descripted in detailed in this writing (section5).

It is difficult to state that the awareness program has reached its objectives without measuring it. Having implemented an information security awareness program does not automatically guarantee that all employees understand their role in ensuring the security and safeguarding of information and information assets. In order for security awareness programs to add value to an organization it is necessary to measure its effect.

The effectiveness level of security awareness Program is assessed right after the awareness Program conduction. The purpose of this, is to remove the oblivion factor that may affect survey results and to identify the level of understanding.

The objective of this survey is to allow employees to provide qualitative response in order to capture employee's sensation regarding awareness and whether they truly exercise security awareness. Survey was conducted anonymously to avoid users not giving honest answers, so the questions were carefully designed to motivate respondents to answer honestly, rather than giving an "expected" answer.

The information security awareness survey was conducted using web-based tools Microsoft Forms in order to examine the effectiveness of the information security awareness program and covered all Security Awareness Program topics: Security Organization, Employee responsibilities, password management, information protection, computer protection, Social engineering, Physical protection, Incident response, equipment protection.

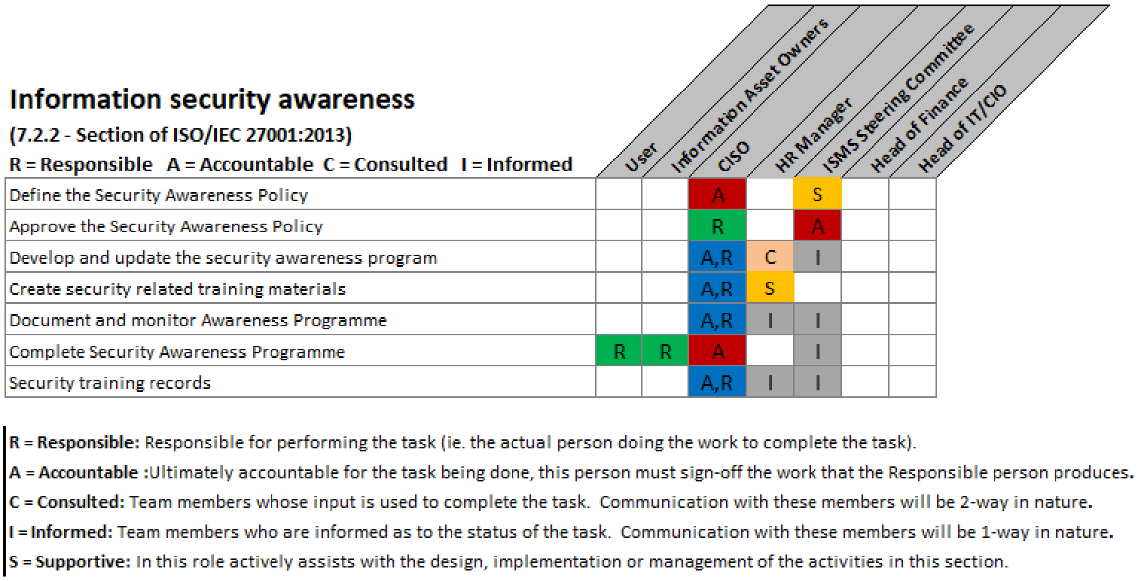
5. Security Awareness Program - Design

Security awareness seeks to focus an individual's attention on an issue or set of issues and should be customised for the specific audience they are targeting. According to "ENISA Information Security awareness guide" [9], there are three processes that should be considered, Plan, assess and design - Execute and manage - Evaluate and adjust. Based on these process Security Awareness Program took place including the bellow sub-processes:

5.1. Plan, assess and Design

5.1.1. Establish Program Team

A team is established to launch the process of awareness Program. The team's main goal is to plan and organise the awareness initiative by completing the tasks foreseen in this phase. Team consist from CISO, HR, IT Manager, Service Delivery Manager. Roles and Responsibilities has been defined in RACI table, *Figure 3*.



Information security awareness

(7.2.2 - Section of ISO/IEC 27001:2013)

R = Responsible A = Accountable C = Consulted I = Informed

	User	Information Asset Owners	CISO	HR Manager	ISMS Steering Committee	Head of Finance	Head of IT/CIO
Define the Security Awareness Policy			A		S		
Approve the Security Awareness Policy			R		A		
Develop and update the security awareness program			A,R	C	I		
Create security related training materials			A,R	S			
Document and monitor Awareness Programme			A,R	I	I		
Complete Security Awareness Programme	R	R	A		I		
Security training records			A,R	I	I		

R = Responsible: Responsible for performing the task (ie. the actual person doing the work to complete the task).

A = Accountable : Ultimately accountable for the task being done, this person must sign-off the work that the Responsible person produces.

C = Consulted: Team members whose input is used to complete the task. Communication with these members will be 2-way in nature.

I = Informed: Team members who are informed as to the status of the task. Communication with these members will be 1-way in nature.

S = Supportive: In this role actively assists with the design, implementation or management of the activities in this section.

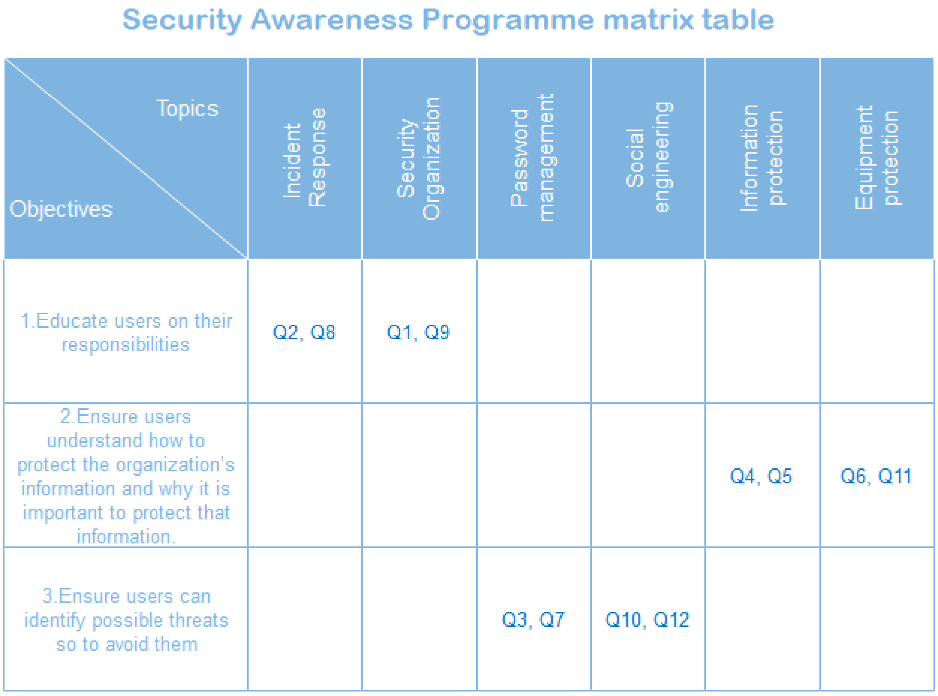
Figure 3: Roles and Responsibilities defined in RACI table

5.1.2. Define Objective

The main Goals of Security Awareness Program is to:

1. educate users on their responsibilities.
2. ensure users understand how to protect the organization's information and why it is important to protect that information.
3. ensure users can identify possible threats so to avoid them i.e. phishing mails, using internet.

Each objective is attached with a set of Security Awareness Program Topic, and each Security Awareness Program Topic is attached with a set of Survey questions. Bellow a matrix table of Security Awareness Program Objectives, Security Awareness Program Topics and Survey questions *Figure 4*.



Security Awareness Programme matrix table

Topics / Objectives	Incident Response	Security Organization	Password management	Social engineering	Information protection	Equipment protection
1.Educate users on their responsibilities	Q2, Q8	Q1, Q9				
2.Ensure users understand how to protect the organization's information and why it is important to protect that information.					Q4, Q5	Q6, Q11
3.Ensure users can identify possible threats so to avoid them			Q3, Q7	Q10, Q12		

Figure 4: Security Awareness Program Matrix Table

5.1.3. Define Target Group

The employees of the company are the population for this survey. All employees have been identified as the Security Awareness audience because of their working nature/responsibility handling customers information (no sensitive). Moreover, there are departments consists of one two or three employees that this expose their anonymity.

Company currently employees' number is 33 people. The e-mail request to participate in the survey was sent to all of them. It is assumed that the group is representative such that there are participants from all working departments, different ages, all genders, different employment contracts.

5.1.4. Security Awareness material

The Internet offers a vast array of information and material available both free of charge and on a fee basis. Several registrations it is done in order to gather all necessary material to achieve Security Awareness Goals. In general awareness materials will be obtained from:

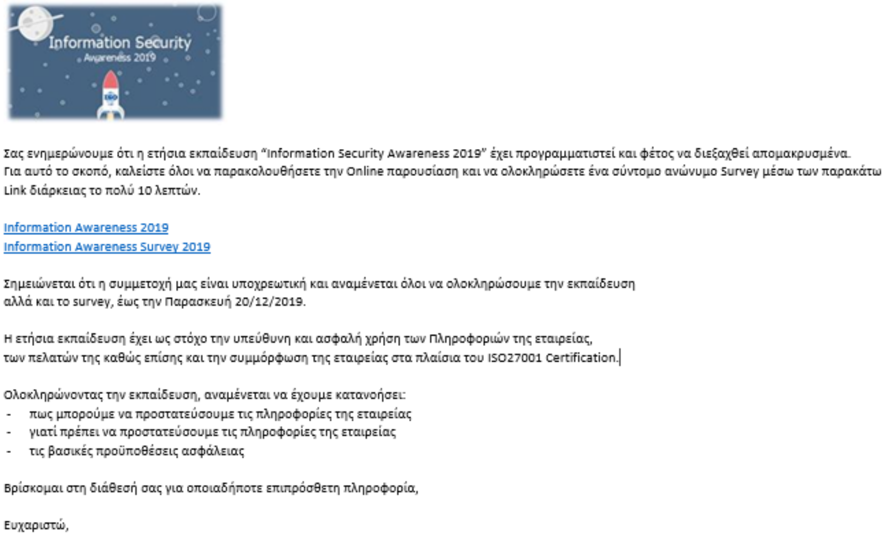
- Internal corporate resources including materials developed and used previously, plus information security policies, standards, guidelines etc.
- Content in the form of presentations, newsletters, posters, briefing papers, checklists, quizzes etc.
- Public information on the Internet e.g. information security incidents and privacy breaches.
- Materials published by the government, industry bodies and others e.g. laws and regulations, information security surveys, guidelines and booklets on privacy.

5.1.5. Obtaining Appropriate Management Support and Funding

Security Steering Committee is the Sponsor of the Security Awareness Program. Budget it is allocated following the Security Awareness Program needs identification (i.e. awareness material).

5.1.6. Define Communications Concept

Effective communication is critical to a Program's success. Through the e-mail communication it is ensured that recipients are fully understand WHY they must participate, HOW to participate, WHO sponsor the Program, WHAT is expected, WHY they are the targeted audience and WHEN the recipient should perform the requested actions. Communication Owner is the CISO *Figure 5*.



Σας ενημερώνουμε ότι η ετήσια εκπαίδευση "Information Security Awareness 2019" έχει προγραμματιστεί και φέτος να διεξαχθεί απομακρυσμένα.
Για αυτό το σκοπό, καλείστε όλοι να παρακολουθήσετε την Online παρουσίαση και να ολοκληρώσετε ένα σύντομο ανώνυμο Survey μέσω των παρακάτω Link διάρκειας το πολύ 10 λεπτών.

Information Awareness 2019
Information Awareness Survey 2019

Σημειώνεται ότι η συμμετοχή μας είναι υποχρεωτική και αναμένεται όλοι να ολοκληρώσουμε την εκπαίδευση αλλά και το survey, έως την Παρασκευή 20/12/2019.

Η ετήσια εκπαίδευση έχει ως στόχο την υπεύθυνη και ασφαλή χρήση των Πληροφοριών της εταιρείας, των πελατών της καθώς επίσης και την συμμόρφωση της εταιρείας στα πλαίσια του ISO27001 Certification.

Ολοκληρώνοντας την εκπαίδευση, αναμένεται να έχουμε κατανοήσει:
- πως μπορούμε να προστατεύσουμε τις πληροφορίες της εταιρείας
- γιατί πρέπει να προστατεύσουμε τις πληροφορίες της εταιρείας
- τις βασικές προϋποθέσεις ασφάλειας

Βρίσκομαι στη διάθεσή σας για οποιαδήποτε επιπρόσθετη πληροφορία,

Ευχαριστώ,

Figure 5: E-mail communication Awareness training and Survey

5.2. Execute and manage

5.2.1. Launch the Program

The execution of the Security Awareness Program will be achieved through company authorized IT Solutions. Specifically, the Security Awareness Material (Documents and Videos) will be broadcasted using *Microsoft Stream Figure 6* which also trailed user activity.

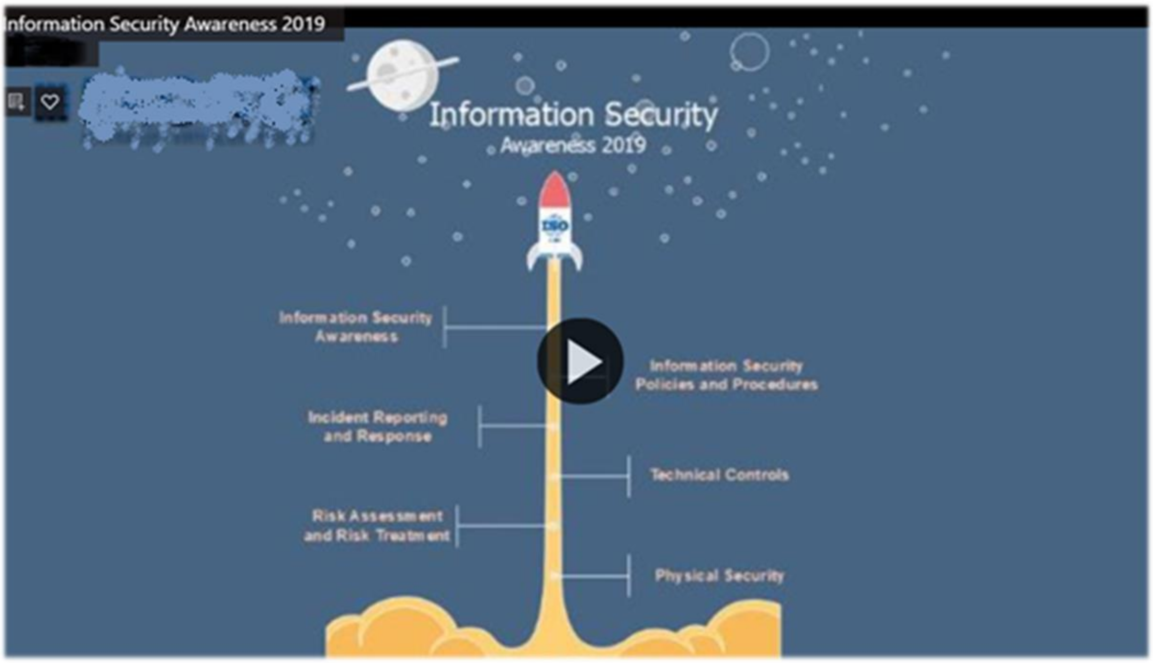

nformation Security Awareness 2019
[redacted]
[redacted]
Information Security
Awareness 2019
Information Security Awareness
Information Security Policies and Procedures
Incident Reporting and Response
Technical Controls
Risk Assessment and Risk Treatment
Physical Security

Figure 6: Security Awareness Material through Microsoft Stream

5.3. Evaluate and adjust

5.3.1. Conduct Evaluations

The effectiveness of an awareness Program and its ability to improve information security have to be measured. The importance of this evaluation is to find out if the objectives of the awareness program is achieved, and what are the results precisely, what are being met, not being met well, or not being met at all for each area of information security.

For this reason, it is decided to execute a relevant survey, questionnaire based. The objective of this survey is to allow employees to provide qualitative response in order to capture employee's sensation regarding awareness and whether they truly exercise security awareness. There are several categories by which security awareness success can be measured. The categories that have been selected are the below:

Process improvement: This category deals with the user understanding of security policies and guidelines based on company ISMS as well as awareness Programs.

Contents of this category are:

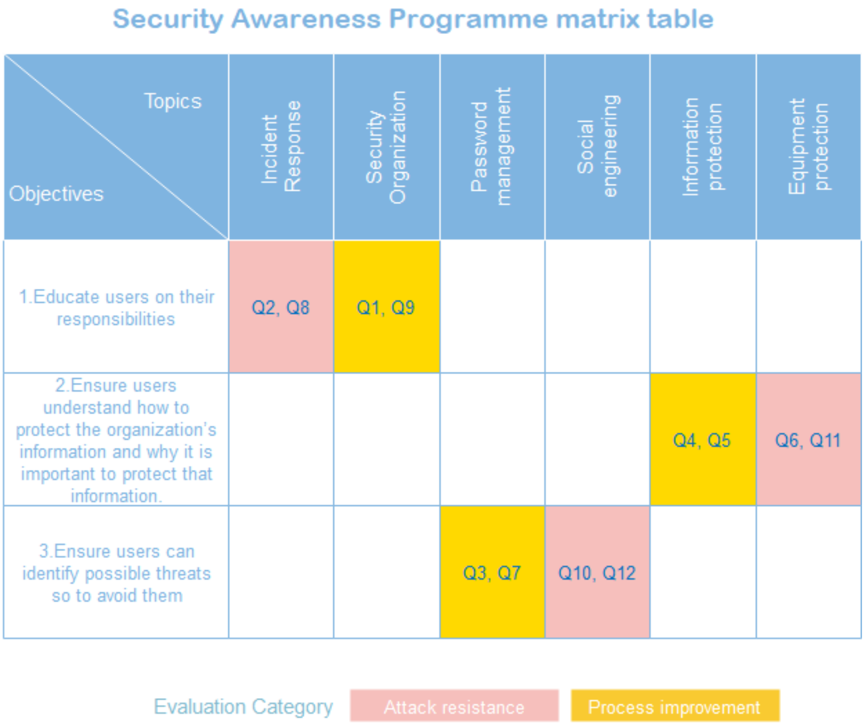
- the percentage of users are confident that they understand the security guidelines. (Q3, Q7).
- the percentage of user know the organization security structure, Policies and Procedures (Q4, Q5).
- the percentage of users keeping customers passwords and personal identification numbers secret (Q1, Q9).

Attack resistance: This category is concerned with the user recognition of a security event and resistance to an attack.

Contents of this category are:

- the percentage of the users recognise an attack, threat or even (Q8, Q10).
- the percentage of users know the correct procedure to follow in case of incident (Q2, Q6).
- the percentage of users are familiar of the Security recommendations (Q11, Q12).

Each question is attached with an Evaluation Category. Bellow a matrix table of Security Awareness Program Objectives, Security Awareness Program Topics, Survey questions and Evaluation Categories *Figure 7*.



Security Awareness Programme matrix table

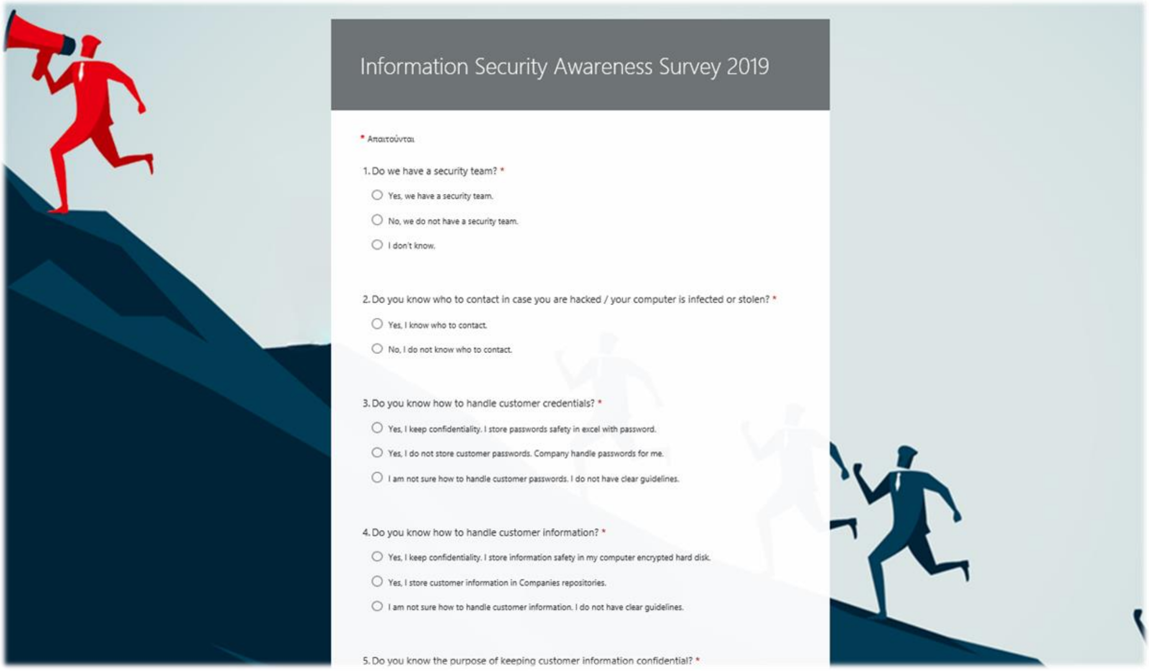
Topics / Objectives	Incident Response	Security Organization	Password management	Social engineering	Information protection	Equipment protection
1.Educate users on their responsibilities	Q2, Q8	Q1, Q9				
2.Ensure users understand how to protect the organization's information and why it is important to protect that information.					Q4, Q5	Q6, Q11
3.Ensure users can identify possible threats so to avoid them			Q3, Q7	Q10, Q12		

Evaluation Category Attack resistance Process improvement

Figure 7: Security Awareness Program Matrix Table

5.3.2. Gather Data

To gather all necessary information in order to evaluate the effectiveness of Security Awareness Program, a Survey (questionnaire) will be achieved through company authorized IT Solutions. Specifically, survey conducted using Microsoft Forms *Figure 8*.



Information Security Awareness Survey 2019

* Απαιτούνται

1. Do we have a security team? *
   - ○ Yes, we have a security team.
   - ○ No, we do not have a security team.
   - ○ I don't know.

2. Do you know who to contact in case you are hacked / your computer is infected or stolen? *
   - ○ Yes, I know who to contact.
   - ○ No, I do not know who to contact.

3. Do you know how to handle customer credentials? *
   - ○ Yes, I keep confidentiality. I store passwords safety in excel with password.
   - ○ Yes, I do not store customer passwords. Company handle passwords for me.
   - ○ I am not sure how to handle customer passwords. I do not have clear guidelines.

4. Do you know how to handle customer information? *
   - ○ Yes, I keep confidentiality. I store information safety in my computer encrypted hard disk.
   - ○ Yes, I store customer information in Companies repositories.
   - ○ I am not sure how to handle customer information. I do not have clear guidelines.

5. Do you know the purpose of keeping customer information confidential? *

Figure 8: Security Awareness Survey using Microsoft Forms

5.3.3. Review Program Objectives

The Program's objectives need to be revisited in light of the effectiveness results in order to be realised if the goal have been achieved or not. If not, it is required to procced in the appropriate actions to achieve the desire result. These actions may include even the re-designation of objectives.

5.3.4. Lessons Learned & Adjustments

Lessons learned can be applied to increase the effectiveness and success of the Program in the future. The main focus is to learn from past experiences both positive and less so, then to put that learning into practice. These actions may include an external company to run awareness sessions even to change the awareness Program method (i.e. Classroom sessions, work around tables, posters, etc) so to invest more in the future Programs. Adjustments should be applied while maintaining the focus on the Program objectives.

6. Security Awareness Program – Effectiveness Survey

Having implemented an information security awareness program does not automatically guarantee that all employees understand their role in ensuring the security and safeguarding of information and information assets. In order for security awareness programs to add value to an organization it is necessary to measure its effect.

For this reason, it is decided to achieve a survey. The surveys are considered to be an excellent tool, for drawing out information from large number of participants, and to make possible the identification of broad tendency [10].

6.1. Survey methodology

Security Steering Committee is the Sponsor of the Security Awareness survey thus the invitation mail to the surveys requesting for participation, is distributed on behalf of the management. The aim of this idea was to get the employees attention, so they dedicate the appropriate attention. It is estimated that all surveys will participate to the survey as it is mandatory.

The information security awareness survey was conducted using web-based tool (Microsoft Forms). The advantage of choosing web-based survey, is because it makes easy statistical analysis of the results and at the same time, employees conducts the survey in their comfortable zone.

Surveys have major speed, minimum cost, and flexibility advantages such as multimedia options (i.e. pictures, videos, colors, etc), multi feature questionnaires such as (no skipped question, randomizations, open fields, anonymization, etc) contrariwise, could be disadvantage since employees could easily quit in the middle of a questionnaire.

The objective of this survey is to allow employees to provide qualitative response in order to capture employee’s sensation regarding awareness and whether they truly exercise security awareness.

Survey was conducted anonymously to avoid users not giving honest answers, so the questions were carefully designed to motivate respondents to answer honestly, rather than giving an "expected" answer. Moreover, there are departments consists of one or two employees that this expose their anonymity

The duration of the survey was focused to keep the completion time around 10 minutes while it was prepared in Greek language containing 12 questions.

Each question has only one right answer that can be selected. Questionnaire is configured to accept only one answer.

6.2.Calculation

This survey consists of 12 questions. Some of the question responses in this survey indicate strong awareness and good security practises while others indicate weak awareness and negligent behaviour. Each question in this survey has been assign a rating value (1-5). “One” is the lowest rating value and “five” is the highest rating value. When the results of this survey have been collected, they can be used to determine the overall Security Awareness Rate reflecting the Security Awareness effectiveness.

Total Response: Each answer rating value (1 – 5) is multiplied by the number of times it was chosen by the surveys.

[Response rating] x [the number of times chosen] = [total response]

Overall Rating: Summary of the Total responses are divided by the number of participants.

[summary of the total response] / [number of surveys] = Overall rating

*minimum rating =12, maximum rating = 60.

Overall Rating Level

Overall Rating Level	Description
Low (<= 20)	Employees are not aware of threats and disregard know security company policies. They engaged in activities or practises that are easily attacked and exploited.
Elevated (<=31)	Employees are not aware of good principles or threats nor they aware of the company policies.
Moderated (<= 42)	Employees are aware of threats and know they should follow good security principles and controls, but they need more training on company security and policies. They also may not know how to identify or report a security event or incident.
Significant (<= 53)	Employees have already been trained on company security and policies, they aware of threats but they may not follow good security principles and controls.
High (<= 60)	Employees are aware of good security principles and threats, have been properly trained and comply with company security and policies.

6.3. Question types

According to "Creative Research System" [10], there are many steps that needs to be followed during the survey questioning such as the meaning of the words and expressions used in the questions, the information the respondents are asked to be able to answer the questions, the scale of the answers the respondents are asked to give.

The survey is achieved, questionnaire contained multiple choices. Some of the questions were answered on a 3-point scale (Yes, No, don’t know) or (True, False, don’t know) while some others used pre-defined answers.

All of the questions from the survey were mandatory. The reason for using extensively mandatory questions, was because there was a need for completed surveys, to be able to analyse and use the results. One of the main points of the data gathering was to measure the effectiveness of security awareness program, thus partially completed surveys would be useless.

Considerations taken into account:

- Question and answer choice order can encourage people to complete the survey. Ideally, the early questions in a survey should be easy and pleasant to answer. These kinds of questions order encourage people to continue the survey.
- The order in which the answer choices are presented can also affect the answers given. The order can make individual questions easier or more difficult to answer. For this reason, answer choices have a natural order 3-point scale (Yes, No, don’t know) or (True, False, don’t know) while some others used pre-defined answers.
- The other way question order can affect results is habituation. This problem applies to a series of questions that all have the same answer choices. It means that some people will usually start giving the same answer, without really considering it, after being asked a series of similar questions. People tend to think more when asked the earlier questions in the series and so give more accurate answers to them. For this reason, we word some statements so that a high level of agreement means satisfaction (e.g., "My supervisor gives me positive feedback") and

others so that a high level of agreement means dissatisfaction (e.g., "My supervisor usually ignores my suggestions"). This technique forces the respondent to think more about each question.

If these basic rules are not considered the survey would lead to misunderstandings of the questions and longer response time, which could lead to a higher drop-out rate.

6.4. Pre-test the Questionnaire

The last step in questionnaire design is to test a questionnaire with a small number of surveys before conducting the main survey. The test survey will be conducted on the same tagged group of people that will be included in the main survey.

This kind of test can reveal unanticipated problems with question wording and help on identifying the level of surveys understanding on the context of questions.

6.5. Survey Questions

The survey questions were organized in the below order.

1. Do we have a security team?
   a. Yes, we have a security team. (5)
   b. No, we do not have a security team. (1)
   c. I don't know (2)

Description: Employees who choose b and c are not informed and pose a risk for obvious reasons.
Objective category: Process improvement

2. Do you know who to contact in case you are hacked / your computer is infected or stolen?
   a. Yes, I know who to contact. (5)
   b. No, I do not know who to contact. (1)

Description: Employees who choose b is potential exposing the company pose a significant risk (breach) because they are likely to continue to use the device.
Objective category: Attack resistance

3. Do you know how to handle customer credentials?
   a. Yes, I keep confidentiality. I store passwords safety in excel with password. (2)
   b. Yes, I do not store customer passwords. Company handle passwords for me. (5)
   c. I am not sure how to handle customer passwords. I do not have clear guidelines. (1)

Description: Employee who choose "b" are well trained and know how to exercise company's security operations. In addition, users who choose "a" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.
Objective category: Attack resistance

4. Do you know how to handle customer information?
   a. Yes, I keep confidentiality. I store information safety in my computer encrypted hard disk. (3)
   b. Yes, I store customer information in Companies repositories. (5)
   c. I am not sure how to handle customer information. I do not have clear guidelines. (1)

Description: Employee who choose "b" are well trained and know how to exercise company's security operations. In addition, users who choose "a" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.
Objective category: Process improvement

5. Do you know the purpose of keeping customer information confidential?
   a. Yes, I know. If I do not keep customer information safe, I may receive a disciplinary action from my boss. (2)
   b. Yes, I know. I implement companies Policies and Procedures to achieve Companies Security strategy and keep company secure. (5)
   c. I am not sure. I am responsible for my actions, in case of mistake i will be exposed not my company. (1)

Description: Employee who choose "b" are well trained and know how to exercise company's security operations. In addition, users who choose "a" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.
Objective category: Process improvement

6. Mobile phones are personal equipment and there is no need to be included in security policies.
   a. No need to implement security on my mobile, moreover I do not allow company to access my personal information. (1)
   b. I am aware that company implement specific security technology to protect only corporate information while at the same time I keep my personal information "only for my eyes". (5)

Description: Employee who choose "a" are not aware regarding company's security measures and privacy policies, are not well trained must be handle with further awareness and training.
Objective category: Process improvement

7. I am aware that i should never give my password to somebody else, however my work is of such a nature that I do give my password from time to time only to a colleague.
   a. Yes, but it is only for business purpose. (1)
   b. I am aware to keep my password secret and I do not pass it to anyone else even if disturbed business. (3)
   c. I am aware to keep my password secret but never happened someone to ask for my password. (5)

Description: Employee how choose "a" and "b", do not understand company policies and strategy. Do not implement security guidelines and best practises, do not protect Service Delivery processes. Need to be trained regarding Security Policy and Company objectives,
Objective category: Process improvement

8. My computer has no value to hackers, they do not target me.
   a. True. (1)
   b. False. (5)

Description: Employee: Users who choose "a" pose a significant risk to the organization because they are unaware of the treat and impact if their computer is compromised.
Objective category: Attack resistance

9. I am aware of the company Policies and Procedures. I know where to look if am not sure for something relevant.
    a. Yes, I am aware, and I know the document location. (5)
    b. Yes, I am aware, but I am not sure I know where the document location is. (3)
    c. No am not aware at all. (1)

Description: Employee: Users who choose "a" are well trained and know how to exercise company's security operations. In addition, users who choose "b" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.
Objective category: Process improvement

10. Have you ever received a phishing mail?
    a. Yes, I have, and I immediately delete it. (5)
    b. No. I am sure outlook filtering phishing mails for me. (2)
    c. I am not sure I have received any phishing mails. (1)

Description: Employee: Employee who choose "a" are well trained and know how to exercise company's security guidelines. In addition, users who choose "b" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.
Objective category: Attack resistance

11. I know how to keep safe my company laptop when I am out of office for business purposes.
    a. Yes, I usually do not leave it unattended. (5)
    b. Yes, I usually store it at the back of my car (3)
    c. I really do not care; it is not my property. (1)

Description: Employee who choose "a" are well trained and know how to exercise company's security guidelines. In addition, users who choose "b" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.

Objective category: Attack resistance

12. Internet access from the company's systems should be used for business purpose only.
    a. Yes, it is only for business purpose. (5)
    b. No, I have access to every site i want. (1)

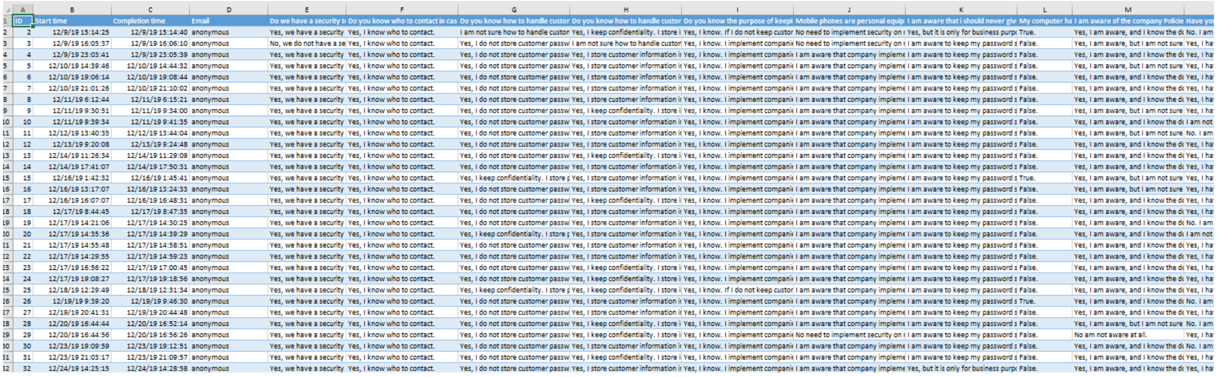
Description: Employee who choose "b" are potential risk for the company, no well-trained and must be handle with further awareness and training.
Objective category: Attack resistance

6.6. Data Analysis

6.6.1. The Response Data

The objective of this survey is to allow employees to provide qualitative response in order to capture employee's sensation regarding awareness and whether they truly exercise security awareness. Survey was conducted anonymously to avoid users not giving honest answers, so the questions were carefully designed to motivate respondents to answer honestly, rather than giving an "expected" answer.

The online survey software "Microsoft Forms" offers the opportunity to export the results from the surveys to Excel sheet in a raw data format *Figure 9*. Excel offers the functionality to analyse data in a pivot table. Data were analysed in a pivot table and then transferred to a secondary Excel sheet *Figure 9*, for chart presentations. Additional software "Edraw Max" was used in order to design an Executive capture of results and conclusions.



	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	ID	Start time	Completion time	Email	Do we have a security t	Do you know who to contact in cas	Do you know how to handle custon	Do you know how to handle custon	Do you know the purpose of keepi	Mobile phones are personal equip	I am aware that i should never giv	My computer ha	I am aware of the company Policie	Have yo
2	2	12/9/19 15:14:25	12/9/19 15:14:40	anonymous	Yes, we have a security	Yes, I know who to contact.	I am not sure how to handle custon	Yes, I keep confidentiality. I store i	Yes, I know. If I do not keep custor	No need to implement security on	Yes, but it is only for business purp	True.	Yes, I am aware, and I know the d	No. I am
3	3	12/9/19 16:05:37	12/9/19 16:06:10	anonymous	No, we do not have a se	Yes, I know who to contact.	Yes, I do not store customer passw	I am not sure how to handle custon	Yes, I know. I implement compani	No need to implement security on	I am aware to keep my password s	False.	Yes, I am aware, but I am not sure	Yes, I ha
4	4	12/9/19 23:03:41	12/9/19 23:05:39	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
5	5	12/10/19 14:39:46	12/10/19 14:44:32	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, but I am not sure	Yes, I ha
6	6	12/10/19 19:06:14	12/10/19 19:08:44	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
7	7	12/10/19 21:01:26	12/10/19 21:10:02	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
8	8	12/11/19 6:12:44	12/11/19 6:15:21	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
9	9	12/11/19 9:30:51	12/11/19 9:34:00	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, but I am not sure	Yes, I ha
10	10	12/11/19 9:39:34	12/11/19 9:41:35	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	I am not
11	11	12/12/19 13:40:35	12/12/19 13:44:04	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, but I am not sure	No. I am
12	12	12/13/19 9:20:08	12/13/19 9:24:48	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
13	13	12/14/19 11:26:34	12/14/19 11:29:09	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
14	14	12/14/19 17:41:07	12/14/19 17:50:31	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
15	15	12/16/19 1:42:32	12/16/19 1:45:41	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I keep confidentiality. I store p	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	True.	Yes, I am aware, but I am not sure	Yes, I ha
16	16	12/16/19 13:17:07	12/16/19 13:24:33	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, but I am not sure	Yes, I ha
17	17	12/16/19 16:07:07	12/16/19 16:48:31	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
18	18	12/17/19 8:44:45	12/17/19 8:47:35	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
19	19	12/17/19 14:21:06	12/17/19 14:30:25	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	No. I am
20	20	12/17/19 14:35:36	12/17/19 14:39:29	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I keep confidentiality. I store p	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	I am not
21	21	12/17/19 14:55:48	12/17/19 14:58:51	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
22	22	12/17/19 14:29:55	12/17/19 14:59:23	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
23	23	12/17/19 16:56:22	12/17/19 17:00:45	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
24	24	12/17/19 19:08:27	12/17/19 19:18:56	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
25	25	12/18/19 12:29:49	12/18/19 12:31:34	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I keep confidentiality. I store p	Yes, I keep confidentiality. I store i	Yes, I know. If I do not keep custor	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
26	26	12/19/19 9:39:20	12/19/19 9:46:30	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	True.	Yes, I am aware, and I know the d	No. I am
27	27	12/19/19 20:41:31	12/19/19 20:44:48	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
28	28	12/20/19 16:44:44	12/20/19 16:52:14	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, but I am not sure	No. I am
29	29	12/20/19 16:44:56	12/20/19 16:56:26	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	No need to implement security on	I am aware to keep my password s	False.	No am not aware at all.	Yes, I ha
30	30	12/23/19 19:09:59	12/23/19 19:12:51	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	No. I am
31	31	12/23/19 21:03:17	12/23/19 21:09:57	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I keep confidentiality. I store i	Yes, I know. I implement compani	I am aware that company impleme	I am aware to keep my password s	False.	Yes, I am aware, and I know the d	Yes, I ha
32	32	12/24/19 14:25:15	12/24/19 14:28:58	anonymous	Yes, we have a security	Yes, I know who to contact.	Yes, I do not store customer passw	Yes, I store customer information i	Yes, I know. I implement compani	I am aware that company impleme	Yes, but it is only for business purp	False.	Yes, I am aware, and I know the d	Yes, I ha

Figure 9: Survey Raw Data through Microsoft Forms

6.6.2. Participation and Completion Results

Firstly, the participation and completion percentage were calculated. The Participation and completion, as it was expected, was massive as the information security awareness Program and Survey was mandatory for all employees. Specifically, the 94% of invitees participate at the information security awareness Program and Survey. The 6% of invitees that did not participate, represent the number of 2 employees that were excused due to approved leave *Figure 10*.

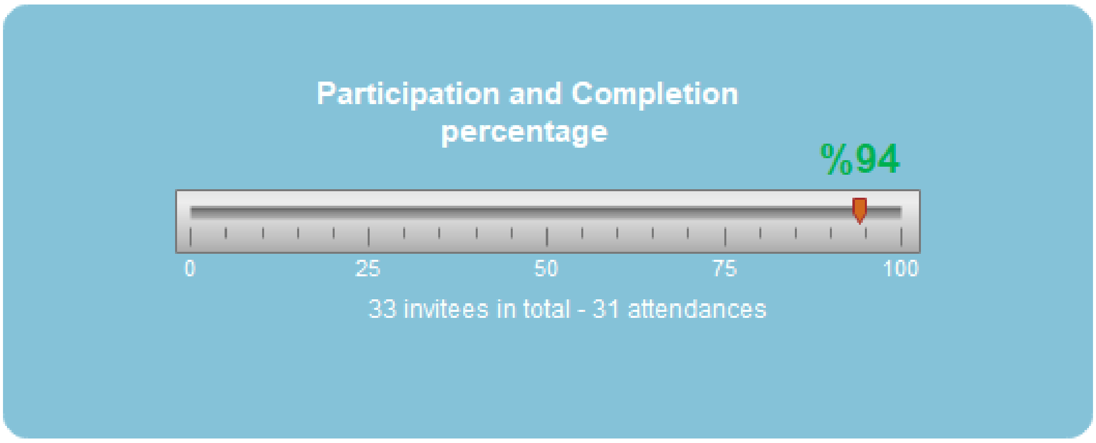


Figure 10: Participation and completion percentage

6.6.3. Grouping and Calculation

Each question was grouped in an Evaluation Category, Awareness Program Topic and Awareness Program Objective and Evaluation Category topic based on 5.1.2 and 5.3.1 section *Figure 11* for further analysis. In a second phase the two categories were analysed based on respond metrics.

For each question were calculated the total number of responses, for each answer (a, b, c). Having the total number of responses per answer, we managed to retrieve the Total Response and the Overall Rating.

Total Response: For each of 12 questions, each question rate value (1 – 5) is multiplied by the number of times it was chosen by the surveys. *Survey minimum rating =12, survey maximum rating = 60.

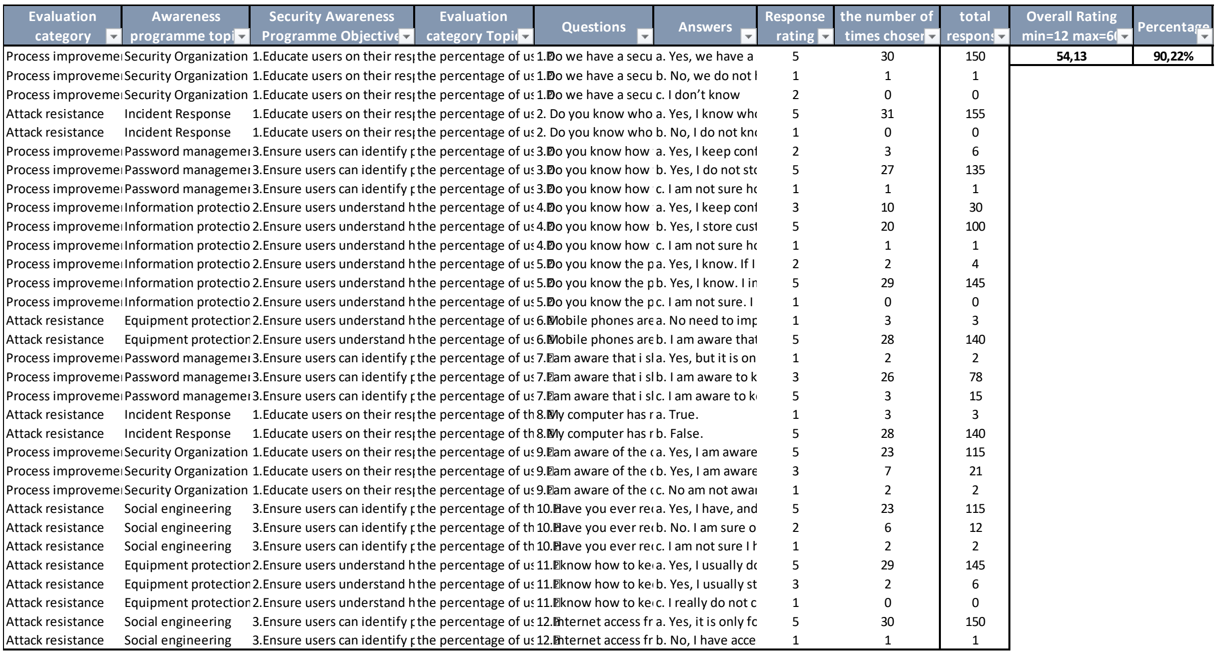
[Response rating] x [the number of times chosen] = [total response]

Overall Rating: Total responses are divided by the number of participants.

[total response] / [number of surveys] = Overall rating

Percentage: Percentage for the Overall Rating result was calculated. The excel cell was formatted in percentage mode.

([Overall Rating Result] / 60) * 100



Evaluation category	Awareness programme topi	Security Awareness Programme Objective	Evaluation category Topi	Questions	Answers	Response rating	the number of times choser	total respons	Overall Rating min=12 max=6	Percentage
Process improveme	Security Organization	1.Educate users on their res	the percentage of us	1.Do we have a secu	a. Yes, we have a	5	30	150	54,13	90,22%
Process improveme	Security Organization	1.Educate users on their res	the percentage of us	1.Do we have a secu	b. No, we do not	1	1	1		
Process improveme	Security Organization	1.Educate users on their res	the percentage of us	1.Do we have a secu	c. I don't know	2	0	0		
Attack resistance	Incident Response	1.Educate users on their res	the percentage of us	2. Do you know who	a. Yes, I know wh	5	31	155		
Attack resistance	Incident Response	1.Educate users on their res	the percentage of us	2. Do you know who	b. No, I do not kn	1	0	0		
Process improveme	Password manageme	3.Ensure users can identify	the percentage of us	3.Do you know how	a. Yes, I keep con	2	3	6		
Process improveme	Password manageme	3.Ensure users can identify	the percentage of us	3.Do you know how	b. Yes, I do not st	5	27	135		
Process improveme	Password manageme	3.Ensure users can identify	the percentage of us	3.Do you know how	c. I am not sure h	1	1	1		
Process improveme	Information protectio	2.Ensure users understand h	the percentage of us	4.Do you know how	a. Yes, I keep con	3	10	30		
Process improveme	Information protectio	2.Ensure users understand h	the percentage of us	4.Do you know how	b. Yes, I store cus	5	20	100		
Process improveme	Information protectio	2.Ensure users understand h	the percentage of us	4.Do you know how	c. I am not sure h	1	1	1		
Process improveme	Information protectio	2.Ensure users understand h	the percentage of us	5.Do you know the p	a. Yes, I know. If I	2	2	4		
Process improveme	Information protectio	2.Ensure users understand h	the percentage of us	5.Do you know the p	b. Yes, I know. I in	5	29	145		
Process improveme	Information protectio	2.Ensure users understand h	the percentage of us	5.Do you know the p	c. I am not sure. I	1	0	0		
Attack resistance	Equipment protection	2.Ensure users understand h	the percentage of us	6.Mobile phones are	a. No need to imp	1	3	3		
Attack resistance	Equipment protection	2.Ensure users understand h	the percentage of us	6.Mobile phones are	b. I am aware that	5	28	140		
Process improveme	Password manageme	3.Ensure users can identify	the percentage of us	7.am aware that i sl	a. Yes, but it is on	1	2	2		
Process improveme	Password manageme	3.Ensure users can identify	the percentage of us	7.am aware that i sl	b. I am aware to k	3	26	78		
Process improveme	Password manageme	3.Ensure users can identify	the percentage of us	7.am aware that i sl	c. I am aware to k	5	3	15		
Attack resistance	Incident Response	1.Educate users on their res	the percentage of th	8.My computer has r	a. True.	1	3	3		
Attack resistance	Incident Response	1.Educate users on their res	the percentage of th	8.My computer has r	b. False.	5	28	140		
Process improveme	Security Organization	1.Educate users on their res	the percentage of us	9.am aware of the	a. Yes, I am aware	5	23	115		
Process improveme	Security Organization	1.Educate users on their res	the percentage of us	9.am aware of the	b. Yes, I am aware	3	7	21		
Process improveme	Security Organization	1.Educate users on their res	the percentage of us	9.am aware of the	c. No am not awa	1	2	2		
Attack resistance	Social engineering	3.Ensure users can identify	the percentage of th	10.Have you ever re	a. Yes, I have, and	5	23	115		
Attack resistance	Social engineering	3.Ensure users can identify	the percentage of th	10.Have you ever re	b. No. I am sure o	2	6	12		
Attack resistance	Social engineering	3.Ensure users can identify	the percentage of th	10.Have you ever re	c. I am not sure I h	1	2	2		
Attack resistance	Equipment protection	2.Ensure users understand h	the percentage of us	11.know how to ke	a. Yes, I usually d	5	29	145		
Attack resistance	Equipment protection	2.Ensure users understand h	the percentage of us	11.know how to ke	b. Yes, I usually st	3	2	6		
Attack resistance	Equipment protection	2.Ensure users understand h	the percentage of us	11.know how to ke	c. I really do not c	1	0	0		
Attack resistance	Social engineering	3.Ensure users can identify	the percentage of us	12.Internet access fr	a. Yes, it is only fo	5	30	150		
Attack resistance	Social engineering	3.Ensure users can identify	the percentage of us	12.Internet access fr	b. No, I have acce	1	1	1		

Figure 11: Survey Data through pivot table in Excel

6.6.4. Responses results

The results of survey responses are presented below for each question:

1. Do we have a security team?
   a. Yes, we have a security team. (5)
   b. No, we do not have a security team. (1)

c. I don't know (2)

Description: Employees who choose b and c are not informed and pose a risk for obvious reasons. Objective category: Process improvement
Results: 97% of total participants respond with a. (best choice) while 3% respond with b. There is no one who respond with c. *Figure 12*
Conclusion: The majority of participants are clearly understanding the Security Organization.

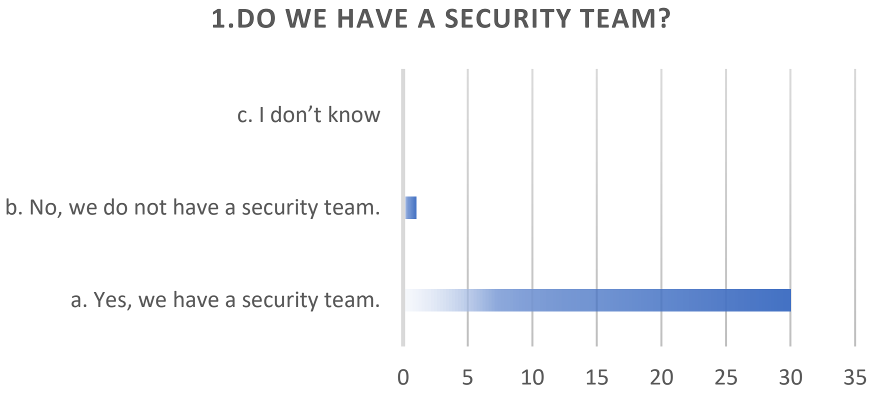


Figure 12: Question 1 responses

2. Do you know who to contact in case you are hacked / your computer is infected or stolen?
   a. Yes, I know who to contact. (5)
   b. No, I do not know who to contact. (1)

Description: Employees who choose b is potential exposing the company pose a significant risk (breach) because they are likely to continue to use the device.
Objective category: Process improvement
Results: 100% of total participants respond with a. (best choice). There is no one who respond with b. *Figure 12.*
Conclusion: The majority of participants are clearly understanding Incident Management Procedure.

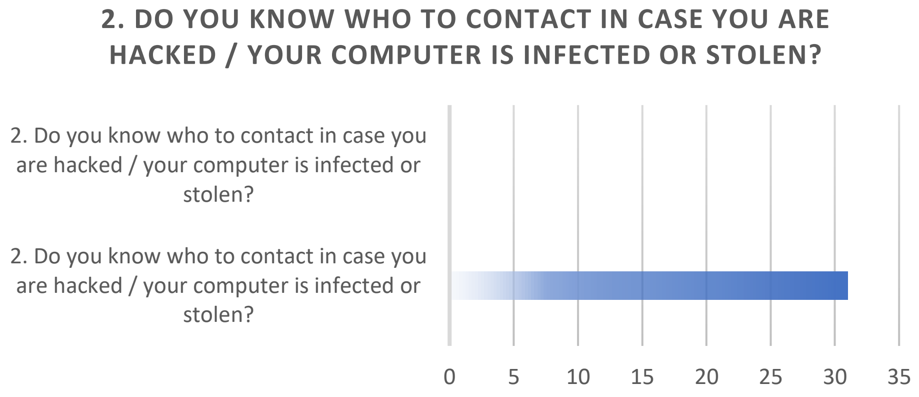


Figure 13: Question 2 responses

3. Do you know how to handle customer credentials?
   a. Yes, I keep confidentiality. I store passwords safety in excel with password. (2)
   b. Yes, I do not store customer passwords. Company handle passwords for me. (5)
   c. I am not sure how to handle customer passwords. I do not have clear guidelines. (1)

Description: Employee who choose "b" are well trained and know how to exercise company's security operations. In addition, users who choose "a" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.

Objective category: Process improvement

Results: 87% of participants respond with b. (best choice) ,10% respond with a. while 3% respond with c. *Figure 14*.

Conclusion: The majority of participants are clearly understanding how to handle Customer Credentials. Although there is a small percentage of users that respond that they do not have clear guidelines, or they store passwords by using non centralize solutions.

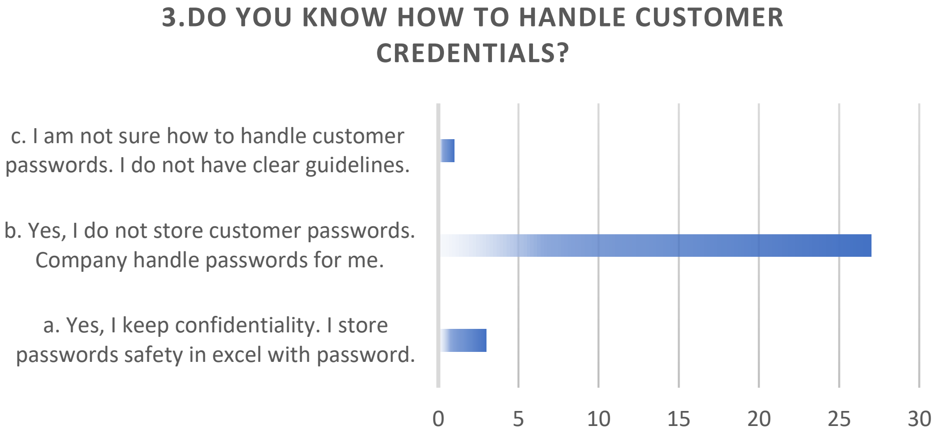


Figure 14: Question 3 responses

4. Do you know how to handle customer information?
   a. Yes, I keep confidentiality. I store information safety in my computer encrypted hard disk. (3)
   b. Yes, I store customer information in Companies repositories. (5)
   c. I am not sure how to handle customer information. I do not have clear guidelines. (1)

Description: Employee who choose "b" are well trained and know how to exercise company's security operations. In addition, users who choose "a" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.

Objective category: Process improvement

Results: 65% of total participants respond with b. (best choice) ,32% respond with a. while 3% respond with c. *Figure 15*.

Conclusion: The majority of participants are clearly understanding how to handle Customer Information. Although there is a small percentage of users that respond that they do not have clear guidelines, or they store customer information by using non centralize solutions.

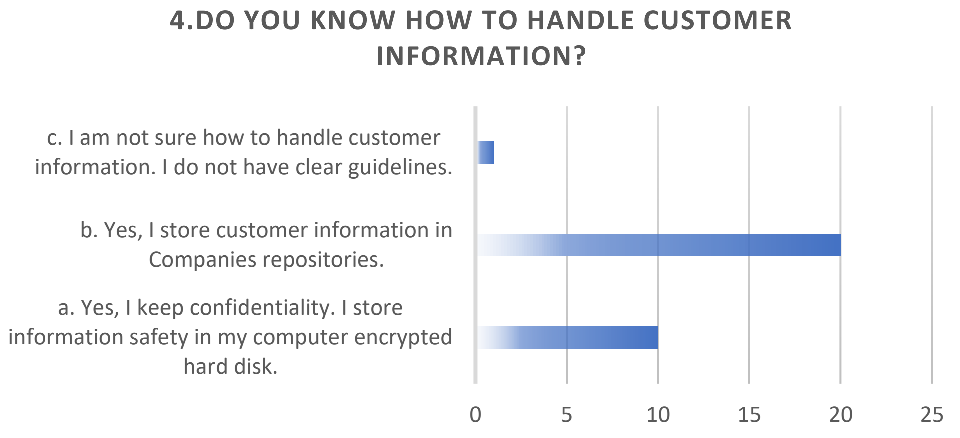


Figure 15: Question 4 responses

5. Do you know the purpose of keeping customer information confidential?
   a. Yes, I know. If I do not keep customer information safe, I may receive a disciplinary action from my boss. (2)
   b. Yes, I know. I implement companies Policies and Procedures to achieve Companies Security strategy and keep company secure. (5)
   c. I am not sure. I am responsible for my actions, in case of mistake i will be exposed not my company. (1)

Description: Employee who choose "b" are well trained and know how to exercise company's security operations. In addition, users who choose "a" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.

Objective category: Process improvement

Results: 94% of total participants respond with b. (best choice) while 6% respond with a. There is no one who respond with c. *Figure 16.*

Conclusion: The majority of participants are clearly understanding why they have to keep customer information confidential. Although there is a small percentage of users that they do not clearly understood the purpose of keeping Confidentiality.

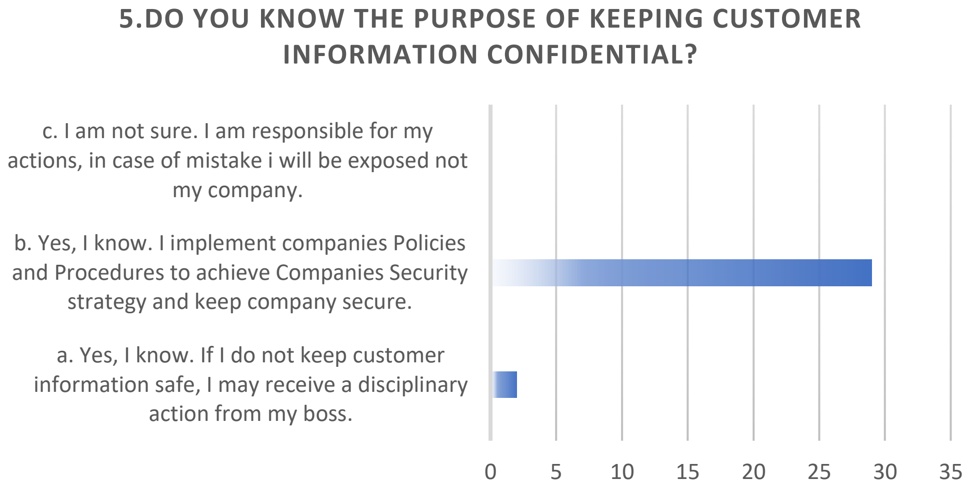


Figure 16: Question 5 responses

6. Mobile phones are personal equipment and there is no need to be included in security policies.
   a. No need to implement security on my mobile, moreover I do not allow company to access my personal information. (1)
   b. I am aware that company implement specific security technology to protect only corporate information while at the same time I keep my personal information "only for my eyes". (5)

Description: Employee who choose "a" are not aware regarding company's security measures and privacy policies, are not well trained must be handle with further awareness and training.
Objective category: Process improvement
Results: 90% of total participants respond with b. (best choice) while 10% respond with a. *Figure 17.*
Conclusion: The majority of participants are clearly understanding about technical controls applied. Although there is a small percentage of users that they do not clearly understood the purpose and the scope of applying technical controls.

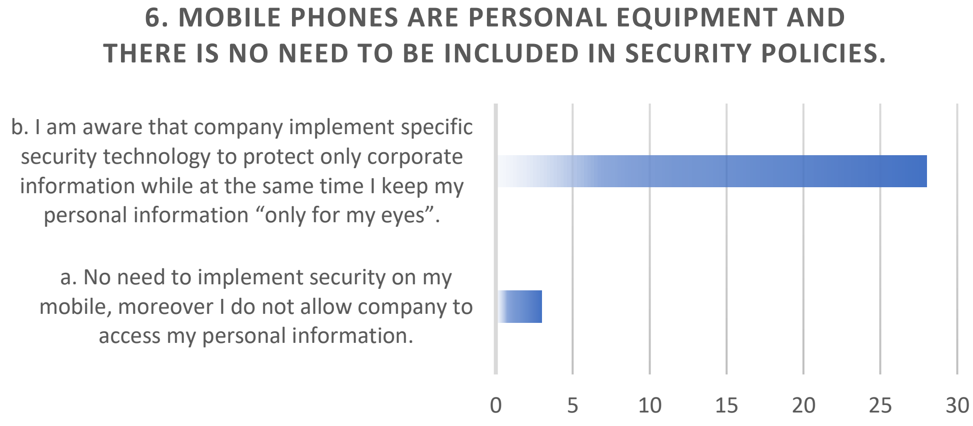


Figure 17: Question 6 responses

7. I am aware that i should never give my password to somebody else, however my work is of such a nature that I do give my password from time to time only to a colleague.
   a. Yes, but it is only for business purpose. (1)
   b. I am aware to keep my password secret and I do not pass it to anyone else even if disturbed business. (3)
   c. I am aware to keep my password secret but never happened someone to ask for my password. (5)

Description: Employee how choose "a" and "b", do not understand company policies and strategy. Do not implement security guidelines and best practises, do not protect Service Delivery processes. Need to be trained regarding Security Policy and Company objectives,
Objective category: Process improvement
Results: 84% of total participants respond with b., 10% respond with c. (best choice) and 6% respond with a. *Figure 18.*
Conclusion: The majority of participants are clearly understanding keeping their password confidential. Although there is a small percentage of users that they are deviate by guidelines.

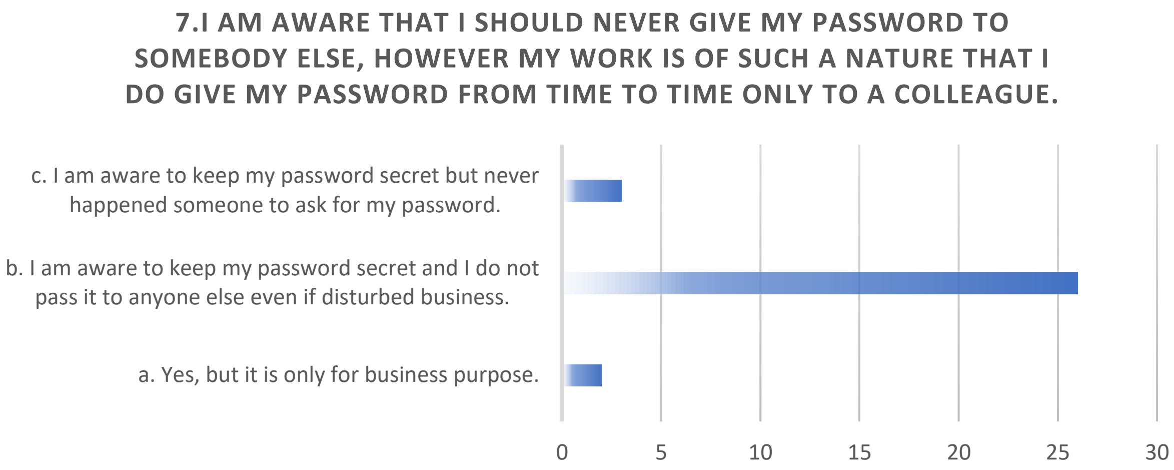


Figure 18: Question 7 responses

8. My computer has no value to hackers, they do not target me.
   a. True. (1)
   b. False. (5)

Description: Employee: Users who choose "a" pose a significant risk to the organization because they are unaware of the treat and impact if their computer is compromised.
Objective category: Attack resistance
Results: 90% of total participants respond with b. (best choice) while 10% respond with a. *Figure 19.*
Conclusion: The majority of participants are clearly understanding that they are a potential target for Security Attacks. Although there is a small percentage of users that they are deviated.

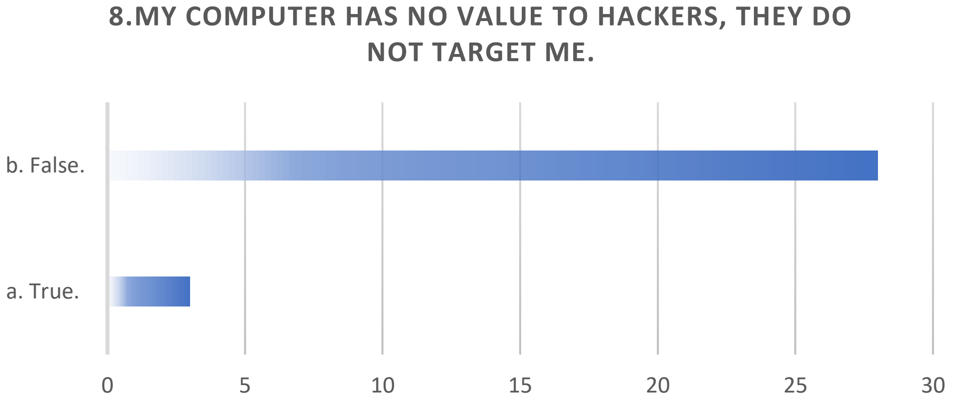


Figure 19: Question 8 responses

9. I am aware of the company Policies and Procedures. I know where to look if am not sure for something relevant.
   a. Yes, I am aware, and I know the document location. (5)
   b. Yes, I am aware, but I am not sure I know where the document location is. (3)
   c. No am not aware at all. (1)

Description: Employee: Users who choose "a" are well trained and know how to exercise company's security operations. In addition, users who choose "b" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.

Objective category: Process improvement
Results: 74% of total participants respond with a. (best choice), 23% respond with b. and 3% respond with c. *Figure 20.*
Conclusion: The majority of participants are clearly understanding about Security Policies guidelines and their repository / location. Although there is a medium percentage of users that they do not clearly understand where they can find the relevant documents, or they did not pay attention at the Awareness section to be informed about Security Policies and their Repository / Location.

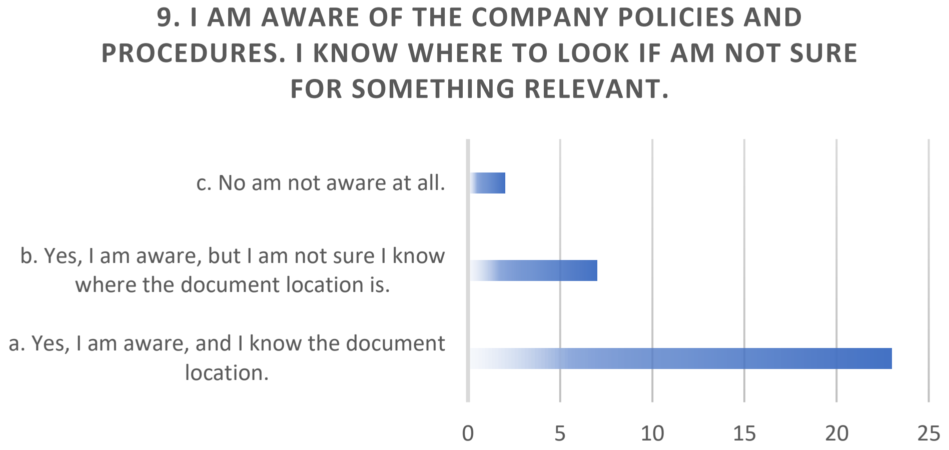


Figure 20: Question 9 responses

10. Have you ever received a phishing mail?
    a. Yes, I have, and I immediately delete it. (5)
    b. No. I am sure outlook filtering phishing mails for me. (2)
    c. I am not sure I have received any phishing mails. (1)

Description: Employee: Employee who choose "a" are well trained and know how to exercise company's security guidelines. In addition, users who choose "b" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.
Objective category: Attack resistance
Results: 74% of total participants respond with a. (best choice), 19% respond with b. and 6% respond with c. *Figure 21.*
Conclusion: The majority of participants are clearly understanding about how to resist on a potential Security attack. Although there is a medium percentage of users that they deviated.

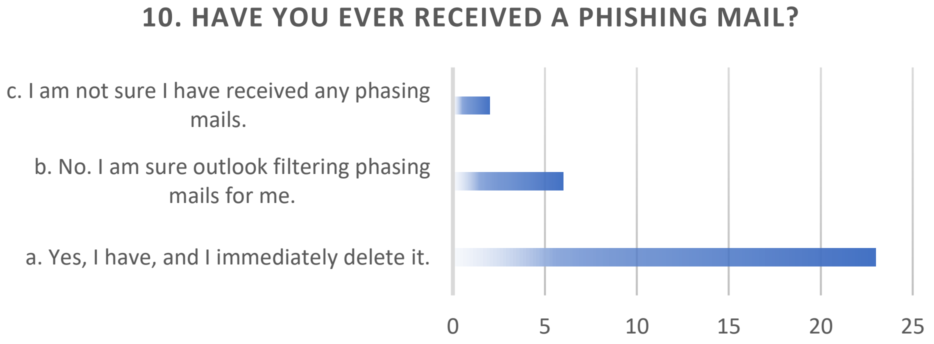


Figure 21: Question 10 responses

11. I know how to keep safe my company laptop when I am out of office for business purposes.
    a. Yes, I usually do not leave it unattended. (5)
    b. Yes, I usually store it at the back of my car (3)
    c. I really do not care; it is not my property. (1)

Description: Employee who choose "a" are well trained and know how to exercise company's security guidelines. In addition, users who choose "b" and "c", are not well trained and therefore pose a significant risk to the organization because they are unaware how to handle security operations.

Objective category: Attack resistance
Results: 94% of total participants respond with a. (best choice), 6% respond with b. There is no one who respond with c. *Figure 22.*
Conclusion: The majority of participants are clearly understanding about how to resist on a potential Security attack (Physical). Although there is a small percentage of users that they deviated.

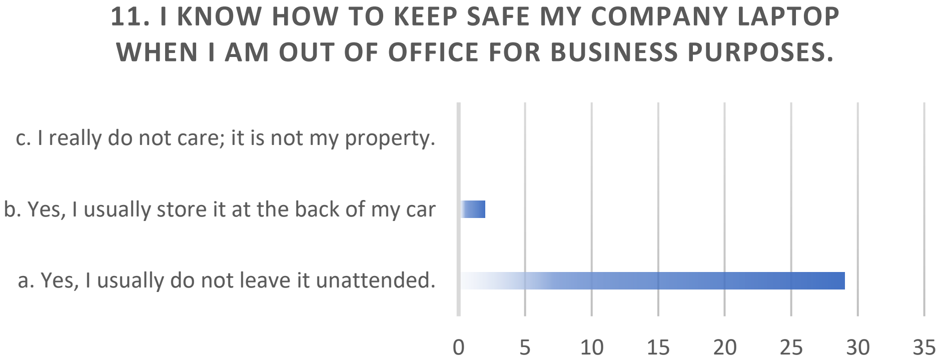


Figure 22: Question 11 responses

12. Internet access from the company's systems should be used for business purpose only.
    a. Yes, it is only for business purpose. (5)
    b. No, I have access to every site i want. (1)

Description: Employee who choose "b" are potential risk for the company, no well-trained and must be handle with further awareness and training.
Objective category: Attack resistance
Results: 97% of total participants respond with a. (best choice), 3% respond with b. *Figure 23.*
Conclusion: The majority of participants are clearly Aware about how to be resisting on a potential Security attack. Although there is a small percentage of users that they deviated.

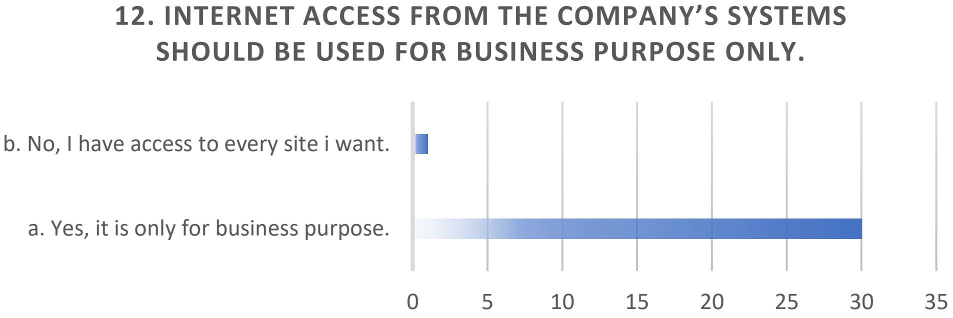


Figure 23: Question 12 responses

6.6.5. Overall Rating

The overall rating reaches almost the 91% *Figure 24*, rising the Rating Maturity scale to "High" meaning that Employees are aware of good security principles and threats, have been properly trained and comply with company's security and policies. As expected, this result is fully satisfactoriness.

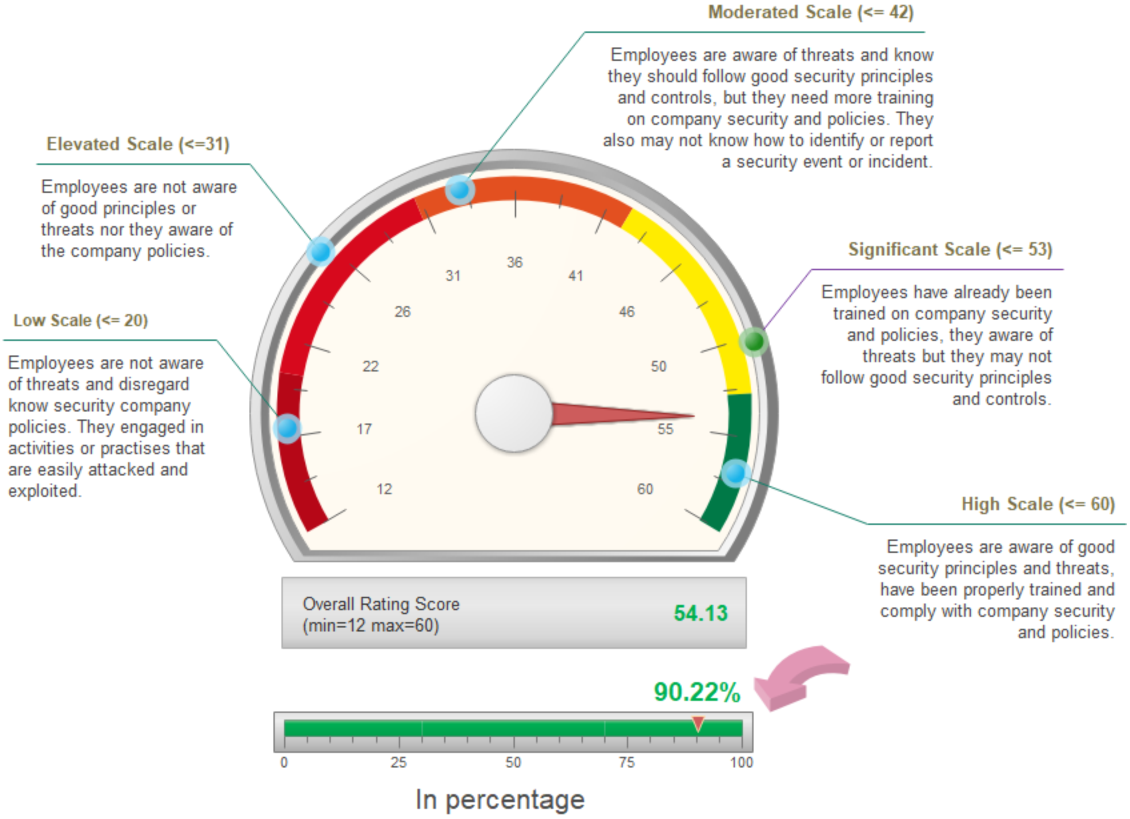


Figure 24: Overall Rating

6.6.6. Evaluation Categories Results

As per section 5.3.1 the evaluation of the effectiveness of Awareness Program is assessed by Categories Process Improvement and Attack Resistance. Following the analysis of Data gathered the score for the Process improvement category represents an achievement score of 87% *Figure 25*.

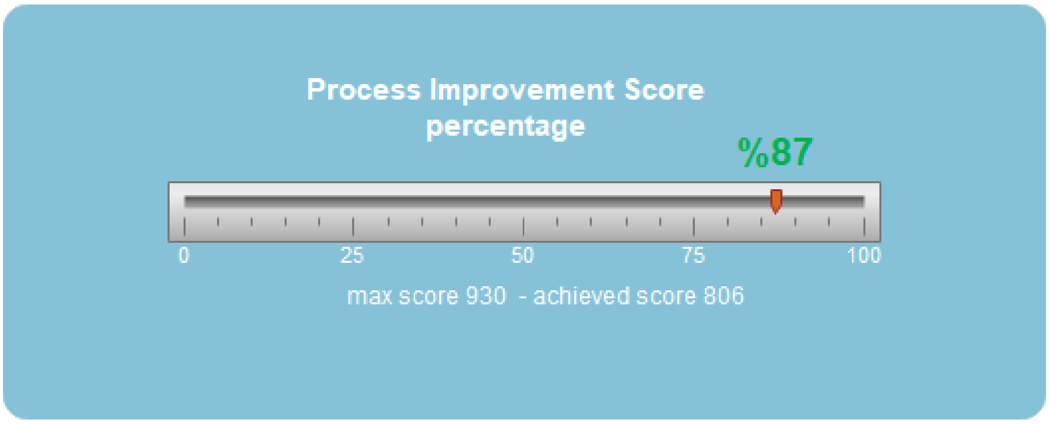


Figure 25: Evaluation Categories Results percentage (Process improvement)

Following the analysis of gathered data, the Process improvement Category by Category content revels that the 90% of employees are confident that they understand the security guidelines, the 93% know the organisation security structure, Policies and Procedures as well as the 76% keep customer passwords and personal identification numbers secret. As it is expected both 90% and 93% are fully satisfactory, in addition the third percentage is not satisfactory and need attention *Figure 26*.

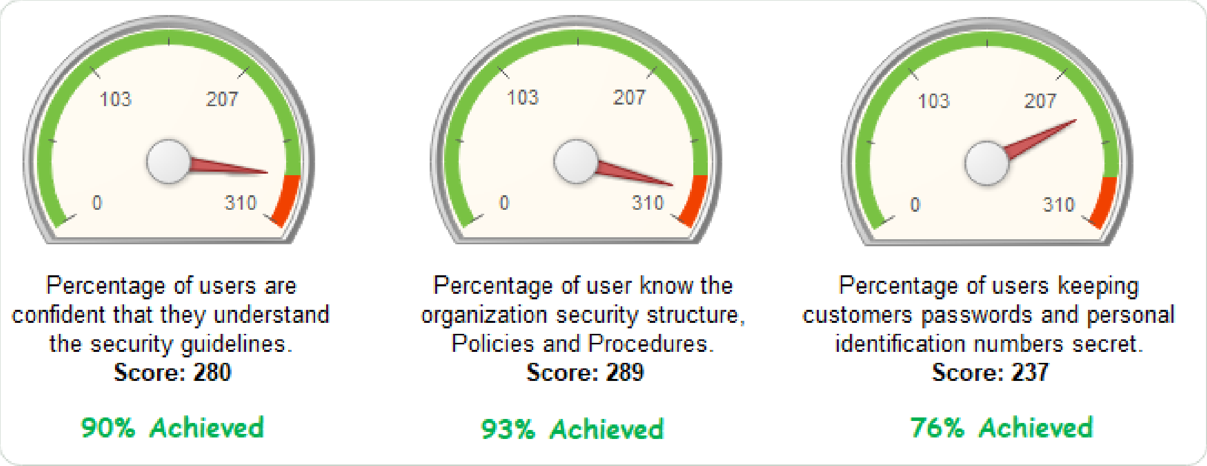


Figure 26: Evaluation Categories Results (Process improvement) per content

Last but not least Attack Resistance category assessed. Following the analysis of Data gathered the score for the Attack Resistance category represents an achievement score of 94% which is satisfactory *Figure 27*.

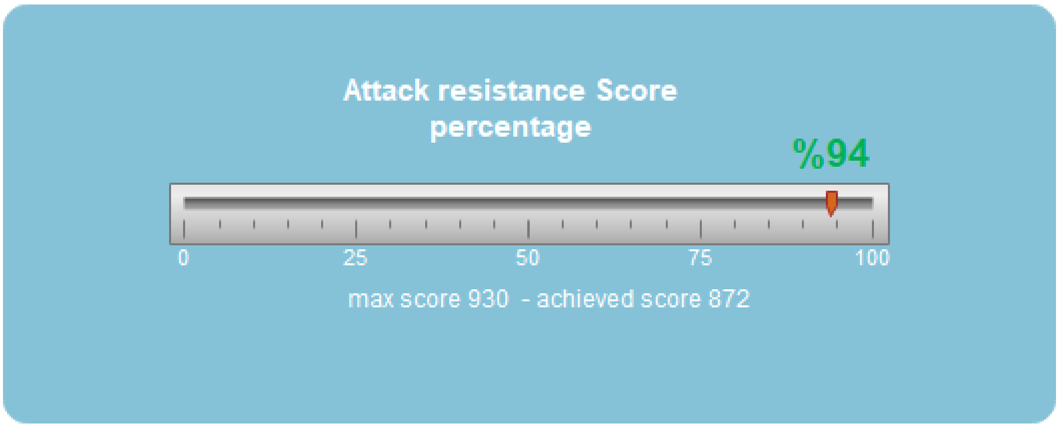


Figure 27: Evaluation Categories Results percentage (Attack Resistance)

Following the analysis of gathered data for the Attack Resistance category by Category content reveals that the 88% the employees recognise an attack, threat or event, the 97% of employees are familiar of the security recommendations as well as the 96% knows the correct procedure to follow in case of an accident. As it is expected both 96% and 97% are fully satisfactory, in addition the third percentage is not and need attention *Figure 28*.

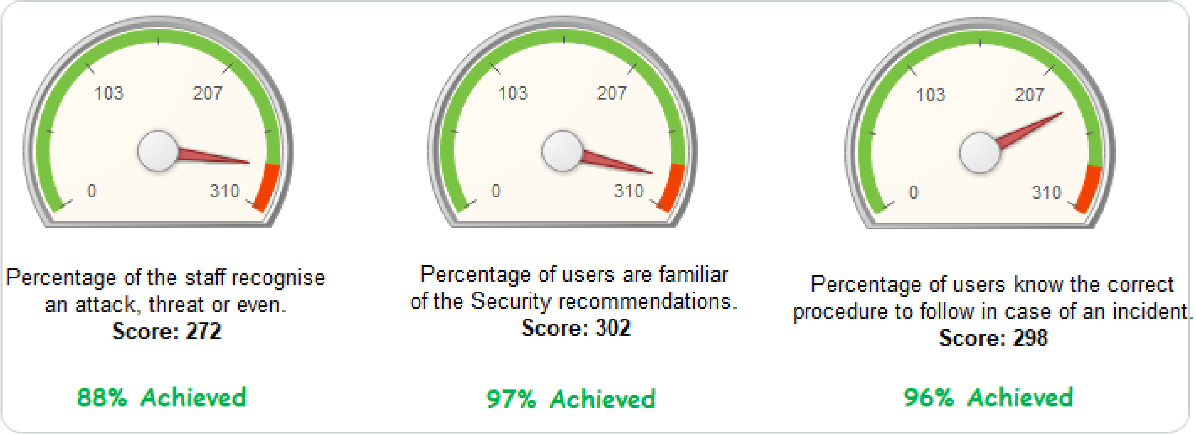


Figure 28: Evaluation Categories Results per content (Attack Resistance)

6.6.7. Security Awareness Program Effectiveness

The evaluation of the effectiveness of Awareness Program is assessed on the Awareness Program Objectives. As per section 5.1.2, the main Goals of Security Awareness Program is to:

1. educate users on their responsibilities.
2. ensure users understand how to protect the organization's information and why it is important to protect that information.
3. ensure users can identify possible threats so to avoid them i.e. phishing mails, using internet.

Each objective is attached with a set of Security Awareness Program Topic, and each Security Awareness Program Topic is attached with a set of Survey questions as it presented on section 5.1.2. As it seams on the F*igure 23* the achievement score for all Objectives are satisfactory, but at the same time, Objective 3 reveals that employees did not reach the same score as the other Objectives and need attention *Figure 29*.

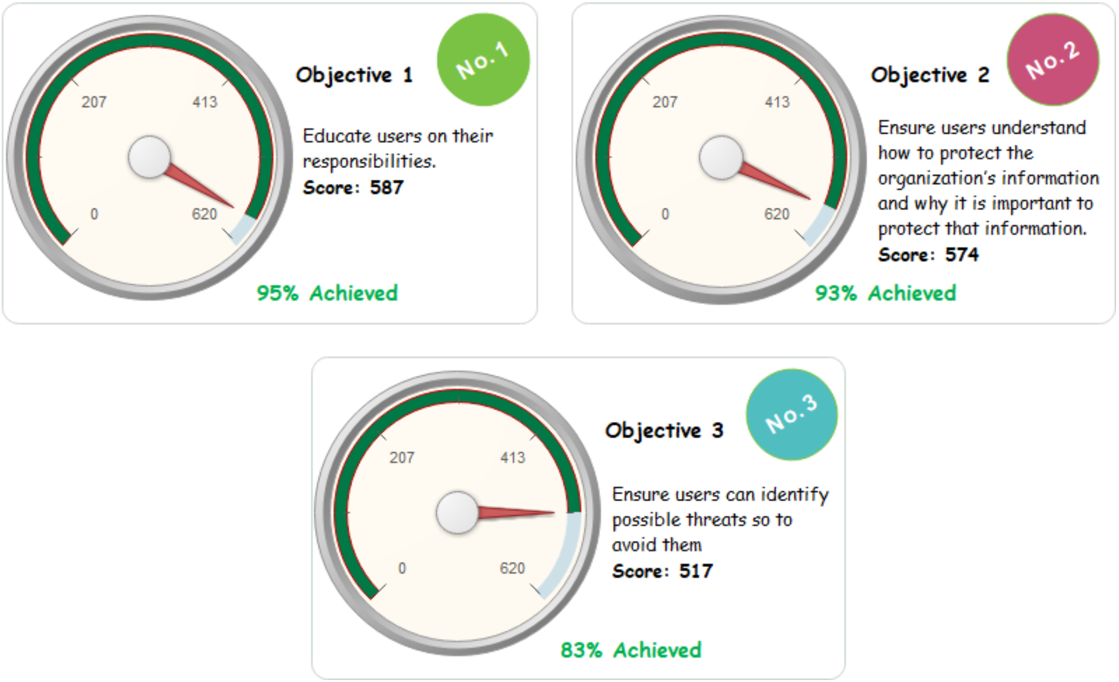


Figure 29: Security Awareness Program Effectiveness per Objective

As per section 5.1.2, Awareness Program Objective is matched with an Awareness Program topic. The analysis of data gathered reveals that the Awareness Program effectiveness reaches the 96% for Incident Response, 95% for the Equipment protection, 90% for the Social Engineering, 93% for the Security Organization and 90% for the Information Protection. Contrariwise, it was not showed the same effectiveness for the Password Management topic representing the percentage of 76% *Figure 30*.

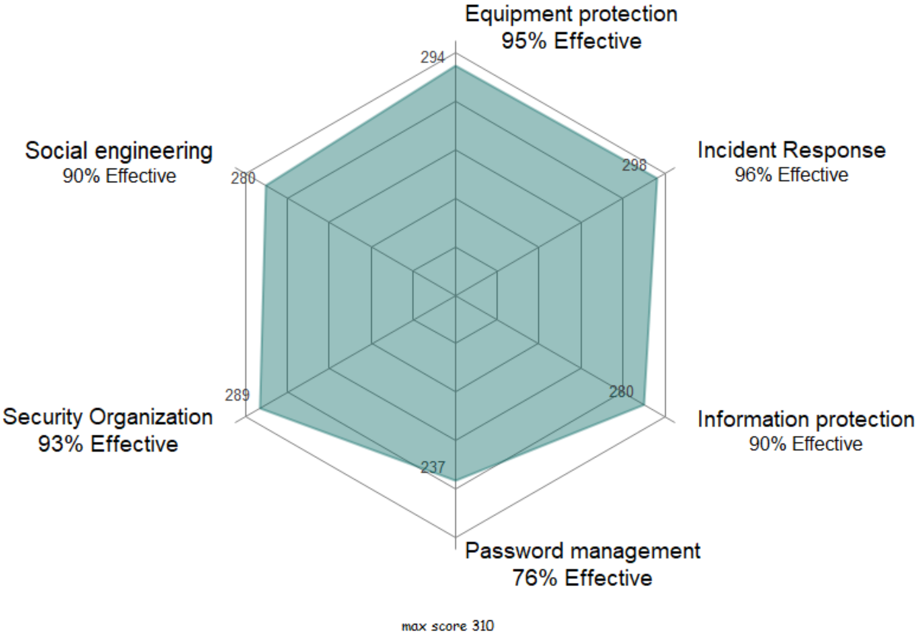


Figure 30: Security Awareness Program Effectiveness per topic

7. Conclusion

Summarizing the overall results, the survey pointed out that the Effectiveness of the Awareness Program is satisfactory reaching the 91% (section 6.6.5), rising the Rating Maturity scale to "High", meaning that Employees are aware of good security principles and threats, have been properly trained and comply with company's security and policies. As expected, this result is fully satisfactoriness.

This Overall result it holds a strong "Value" due to of the massive participation of employees 96% (31 of 33 employees participate in Awareness Program and Survey). Based on that it is strongly believed that management support enforces the employees into a massive participation, since none of the training method would work without participants.

On the other hand, based on data analysis presented in section 6.6, there are some areas that need attention as they effect Objective number 3 and both Evaluation Categories:

Evaluation Categories: The data analysis (section 6.6.6) represents that the Process improvement Category did not achieve a score such as the Attack Resistance Category (87<94). The further Analysis showed that the Process Improvement Category content "users keeping customers passwords and personal identification numbers secret" that is related with Security Organization Awareness topic got a percentage of 76% of achievement, impacting the total Score of Process Improvement Category. Additional study on the results shows that another Evaluation category content for the Attack Resistance Category achieve the 94% effectiveness percentage which is satisfactory. Particularly, the content "employees recognises an attack, threat or event" that is related with Social engineering Awareness topic and Incident Response, reached the score of 88% which is

significant lower than the other two in the same Evaluation Category 97% and 96%. Going deeper into data analysis to reveal the cause of this failure, we notice that the employees did not "pass" the question numbers Q8 and Q10
Q8: My computer has no value to hackers, they do not target me.
Q10: Have you ever received a phishing mail?
.

Awareness Program Objectives: Analysis regarding the Objectives achievement reveals that the Objective number 3 "ensure users can identify possible threats so to avoid them i.e. phishing mails, using internet) did not met the same scores as the other two Objectives (83%< 95%, 93%). Looking carefully in the data analysis, we conclude that the reason that the Objective number 3 did not achieve a score as high as the other two, was the low percentage of Password Management content that was significantly lower than the others (76% < 96%, 95%, 93%, 90%, 90%). Going deeper into data analysis to reveal the case of this failure, we notice that the employees did not "pass" the question numbers Q3 and Q7.
Q3: Do you know how to handle customer credentials?
Q7: I am aware that i should never give my password to somebody else, however my work is of such a nature that I do give my password from time to time only to a colleague.

Analysing the "failed" question responses we ended that:

- 13% of employees does not understand clearly the guidelines, or they prefer to store passwords by using non centralize solutions (Q3).
- 16% of employees may time to time give their password to a colleague for business reasons (Q7).
- 25% of employees are not sure if they ever receive a spam mail or believe that antispam system filters all spam mails (Q10).
- 26% of employees clearly understand security organization but they are not sure where to find information such as Policies and procedures(Q9).
- 3% of employees do not clearly understand the Security Organization (Q1).

It is clearly understood that based on the failure responds on these questions, it is needed to enforce stronger Awareness on these topics and maybe to re-adjust the Awareness Program method from "Web based" to other methods such as classroom or either to extent the Program with Posters, Screensavers, News Letters.

8. Limitations

At the beginning of this thesis it was very clear that it is mandatory a "real" exercise to be achieved. Information's written in this paper had to be real and accurate. It was very clear also that exercises coming with this paper, had to be part of my real working hours as the goal was to simulate the methodology in a working environment. First it seemed possible, but during the paper exercise, it came out that a structured Awareness Training methodology is demanding extra working hour. This was the very first difficulty it was noticed and handled dedicating extra personal time to achieve an accurate result to be presented in this paper. Post -thinking comes with alternatives, such as external services for delivering the awareness material, that results with an extra budget for the company.

A second difficulty were identified after the completion of the Information Awareness Program which are strongly recommended to be improved in the future. Because of the type of survey (conducted anonymously), it was not possible to follow-up the survey with a training session of the individuals who did not pass the survey. On the other hand, if the survey was conducted nominative then there was a real case, employee not giving honest answers and so the result of the survey did not reflect the real Security Awareness Maturity score. A solution may be to alternate the survey methodology each year in order to be able to measure both results with and without anonymity parameter. It is considered that both anonymity and nominative surveys, are equally useful, each for a different perspective.

Another difficulty is that employees have different learning styles [14], listening or reading, visuals – board, video or flipcharts, kinesthetic - learning by doing, feeling, trying it out. A good Awareness training should be a mixed of these types so to reflect a higher Information Security Awareness Maturity Score. People usually are more comfortable in one of these learning styles. A solution could be employees to be able to choose the method that is best for them. On the other hand, this solution demands extra budget.

Summarising all the above, it is mandatory to improve Information Security Awareness Program with parameters such as learning styles, nominative surveys and to proceed on a cost benefit analysis such as time plus the costs for generating and delivering awareness materials (primarily staffing costs external assistance, subscriptions, etc).

9. Bibliography

[1] – Section 7.3, clause A 7.2.2 https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, (last visited on 2/11/2019)

[2] - Implement a Security Awareness CIS - https://www.cisecurity.org/controls/implement-a-security-awareness-and-training-program/, (last visited on 2/11/2019)

[3] – Payment Card Industry (PCI) Data Security Standard V3.2, requirement 12.6 section, (last visited on 2/11/2019)

[4] -European Cyber Security Month (ECSM) - https://cybersecuritymonth.eu/about-ecsm/whats-ecsm, (last visited on 2/11/2019)

[5] - SANS, 2019 Security Awareness Report - https://www.sans.org/security-awareness-training/reports/2019-security-awareness-report, (last visited on 2/11/2019)

[6] - 2019 Symantec Internet Security Threat Report , https://www.symantec.com/security-center/threat-report, (last visited on 2/11/2019)

[7] – Verizon 2019 Data Breach Investigations Report - https://enterprise.verizon.com/resources/reports/dbir/[7] - https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport, (last visited on 2/11/2019)

[8] - EY Global Information Security Survey 2018–19, https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf, (last visited on 2/11/2019)

[9] - ENISA Information Security awareness guide - https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport, (last visited on 9/11/2019)

[10] - Creative Research Systems - https://www.surveysystem.com/sdesign.htm#goals, (last visited on 9/11/2019)

[11] – ENISA Cyber Security Culture in organisations, NOVEMBER 2017, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport

[12] – ENISA Good_practice_guide_on_training_methodologies, November 2014, https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies/at_download/fullReport