AFKC
Value-Added Distributor

WHITE PAPER

SECURITY AWARENESS

Why it is important to build behavior, not just providing knowledge

TABLE OF CONTENTS

1. INTRODUCTION

The great importance of training and knowledge within the company is a long-established concept; too often, however, such knowledge is focused exclusively on the company's core business and on its production cycles.

The quick evolution of IT tools, their pervasiveness within all company functions and the emergence of increasingly frequent and complex threats have introduced a new critical factor related to their use.

Until now, companies have tried to oppose these threats by investing more in infrastructure security technologies to protect company boundaries from attacks coming from the outside, and less in solutions and processes that oppose the loss of information (see also the focus on this theme contained in the recent European legislation "GDPR").

Even more rarely companies care about planning employee training aiming to improve awareness in the use of corporate information technology tools and the information they process and contain. This type of intervention must be extended to all employees, with greater attention to those who do not play a role in ICT or in internal security. Adopting such approach can lead to significant reductions in security incidents, whose origin is inattentiveness and superficiality and which represent a significant percentage of the total.

2. CYBER INCIDENTS WITHIN COMPANIES

Nowadays, most of Cyber Incidents (80%) which verify within companies are imputable to human errors (statistics coming from different sources on the market show that this percentage ranges between 70% and 80%, and so we are dealing with pretty shared data). Actually, Cyber Incidents are not being caused by inadequate infrastructures and security technologies (where investments are often concentrated), but simply by an unaware users' behavior; we're talking obviously about users who do not belong to the IT/security sector. Most of the time we deal with behavior occurring also outside of the corporate environment, where perimeter defenses cannot compensate threats, and devices are more easily hackable.

Unfortunately, the same superficiality is applied by users on their personal devices, resulting in damages which may lead to the abduction of information such as personal credentials, bank data, etc.

It is widely known that most of these incidents are not made public for a series of reasons (mainly linked to the reputation of the firm): such behaviour makes sharing information about threats and building a common strategy to contrast them more difficult, thereby favouring their diffusion. Without any doubt, the conformity to European GDPR normative will help organizations to treat correctly information risk and to manage related security incidents.

In order to have a reference point on the issue of economic losses related to security incidents, we shall consider that phishing attacks only (e-mail messages containing links to compromised sites or damaging attachments) cost to companies an yearly average of 400€ per employee.

FIG.1

Why is security awareness so important?

3. BUILDING AN EFFECTIVE SECURITY AWARENESS STRATEGY

3.1 Training Approach

Traditional classroom-based training, with classic daily modules, have demonstrated to be completely useless in reaching planned objectives; the complexity of the subject, the low interest that these issues create among employees, and also the use of traditional education techniques no longer adequate are among the causes of this lack of success.

Most recent researches have demonstrated that a greater effectiveness can be reached through multiple techniques:

- Training modules with a length of max 30 minutes (consecutively)
- Detailed arguments
- Quizzes inside modules, to verify a correct understanding of the subject, before passing on to the next one
- Questions backed up with effective and exhaustive feedback on the answer provided by the user
- Appealing language and graphic

Appropriate awareness and training courses may be difficult to integrate in the everyday life of a business. To overcome organizational problems, training should be able to:

- Grant on-line availability
- Allows users to pause a single module at any moment and resume it later
- Grant availability everywhere and every time, in order to meet personal and working obligations of employees

3.2 Objectives

What are the main objectives that a Security Awareness campaign shall reach?

The most important thing to highlight in the Security Awareness courses is that they don't have the sole purpose of training the personnel and make them pass with positive scores, but rather of making them change their overall behaviour. A Security Awareness training campaign can be considered efficient only when, at the end of the year, the number of cyber incidents within a company has significantly decreased.

The second goal to meet is to emphasize in detail which are the risks related to users' wrong behaviors, and evaluate which are the right countermeasures to adopt in order to reduce them. This operation becomes increasingly efficient if confronted with threats present on a company level, on a market level, or on a geographic position level.

Once all the risks related to wrong behaviours have been identified, it is possible to make more efficient investments, at a general, professional and technological support level.

FIG.2
Return of Investments in Cyber Security Awareness

3.3 Security Awareness as a Process

Employee training, and in particular cyber security training, cannot be managed as a project. In other words, you cannot have the ambition to modify some radicated users' habits with just one informative campaign.

Cyber security training, just like cyber security itself, must be managed as a process, that is a series of initiatives which have to be repeated regularly along time, and which have to be followed consistently by moments of evaluation.

In order not to lose their effectiveness, the trainings available need to be continuously adapted to the ever-changing landscape of IT and Cyber threats. The main factors driving these changes are:

- **Evolution of threats:** Attack techniques projected by criminal organizations to break into firms are continuously evolving.
- **Technological progress:** Employees are given more and more IT devices and services to use, which can represent a driver for attack.

- **Personnel mobility:** Employees increasingly find themselves operating out of the company's perimeter, and this makes them more exposed, not being protected by the company's security infrastructures.
- **Exchange of information with stakeholder:** Companies are facing an increasing need of exchanging information with suppliers, customers, partners, etc

4. HOW A SECURITY AWARENESS PROCESS SHOULD BE STRUCTURED

FIG.3

The phases of a well structured Security Awareness Process

4.1 Assessment

The first activity to be performed, before launching any training campaign, is certainly that of making an Assessment. Every CISO of every company needs to have a deep understanding of the base competency of the company personnel, which behavioral mistakes they are responsible for and which risks their behaviour might lead to.

The only way to have a realistic picture is to structure one or more assessment campaigns. The simplest and most efficient way is that of initially submitting consecutive surveys to employees.

Survey should have the following characteristics:

- Not too many questions at once; this may lead the user to get immediately tired and start formulating answers without the right level of attention.
- No survey should cover too many different issues at the same time, in order to allow the users to focus their attention on a few key arguments at a time.
- Questions must be not just about the way IT devices are used, but also about how their usage should adapt depending on the environment: within the company, abroad, in public places, at home, etc.
- Feedback. It is crucial for every answer to be followed by a feedback on the fairness and the reasoning to do. Too often it happens that a user gives a correct answer, still making a wrong reasoning.
- It must be possible to associate a multiple true/false answer to every question.

4.2 Training

Customized training campaigns must be structured based both on the outcome of Assessments campaigns and on the critical issues linked to the single user's role.

Even in this case there are some best practices to follow in order to make this phase more efficient:

- Every training campaign shall comprehend a limited amount of training modules. This helps to avoid generating confusion in the user or lowering his level of attention.
- Every single training module shall have a limited duration (max 15-20 mins). If a subject results to be too broad, it is better to divide it in chapters.
- It is preferable to plan a training programme diversified by user. The priority of chosen modules has to be customized according to criteria such as organizational unit, role, corporate level, single risks exposition, etc.
- It is important that the graphic and interactive interface of single modules trigger users' curiosity and keep them interested in the course.
- Training pages of every module should be spaced with evaluation checkpoints featuring exercises and tests, in order to verify the user's undertstanding of an subject, before passing on to the next one.
- It must be possible to radically change the order of questions proposed to the user, in order to avoid their memorization.

4.3 Evaluation

At the end of the training phase it is essential to go through an evaluation phase, to verify that the training component has been correctly understood by users. Too often, the successful overcoming of a course does not mean that a specific behavior has become natural. This phase can be implemented through different methodologies: using surveys focused on behavioral aspects, or with "attack simulation" tests, (e.g. fake phishing e-mails).

4.4 Analytics and Reporting

A key moment of the Security Awareness process is the collection and analysis of results, of both the Assessment and Training phases. It will be important to be able to see the results both in an aggregated pattern (choosing time by time the aspects to observe) and in detail. Analysis must not be only quantitative (how many have passed the tests or ultimate training modules), but also qualitative; for instance, even if a test has been generally overcame, it is important to know if many users share the same failed questions, in order to be aware of the presence of shared shortcomings or misconceptions among the employees and their danger level for the company.

4.5 Organizational Collaboration

To ensure that the process of Security Awareness is efficient, it is crucial to have a close collaboration among the several Organizational Units involved within the company: HR, Legal, CERT, Security, Governance, ICT, etc.
Irrespective of who will physically manage the platform (usually IT Security or the "education" department of HR) it is necessary for each and every one of OU mentioned above to feel directly engaged in the identification of methodology and in the choice of priorities, and to give its proactive contribution to the process.

5. KASPERSKY EMPLOYEE SKILLS TRAINING PLATFORM

Kaspersky Employee Skills Training Platform is a platform born for Security Awareness, which collects all the features necessary to reach the goals and fullfill the requirements seen before. Its main difference from other general e-learning platforms on the market relies in having the main goal to identify and correct non-appropriate behaviour related to the use of IT instruments and in pursuing such goal with specifically designed functionalities, in order to lower the Cyber incidents within the company,.
This is an on-line platform where the training modules can be exploited in any condition compatible with personal or corporate organization.

5.1 Main Features of Kaspersky security Awareness platform:

- The platform addresses to all company employees, irrespective of their role and their specific competences in the security field.
- All surveys and training modules of the platform are available in 27 different languages.
- Notification system: the platform is able to send (customizable) notifications to users by e-mail, after the occurrence of certain events: registration to a course, registration to an assessment, deadline reminder, etc.
- Users and group management by both interactive and batch (through csv file) mode; ability to interface with corporate authentication platform.

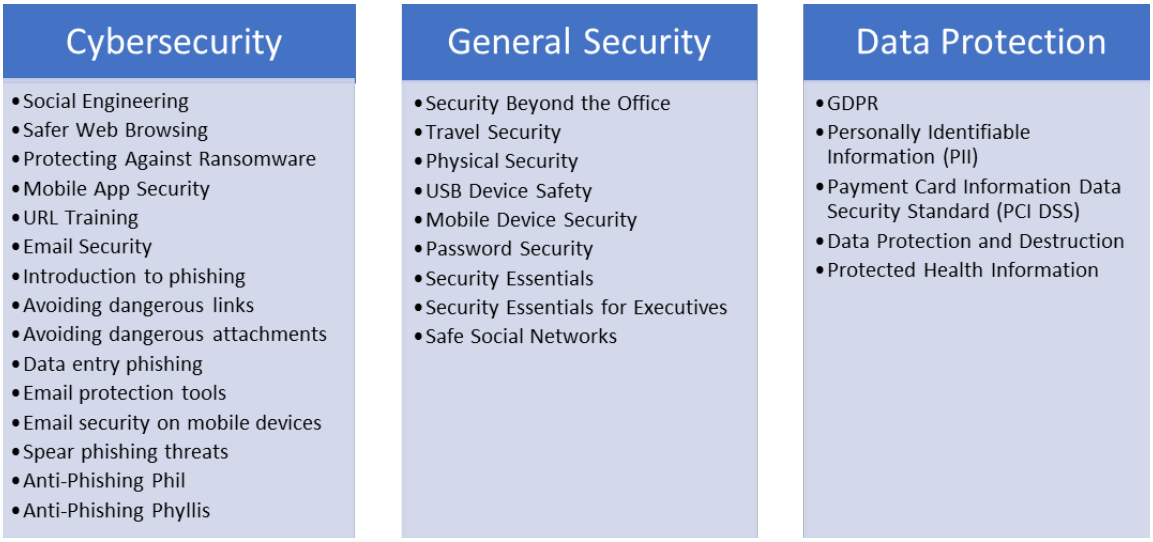
5.2 Characteristics of the assessment component

- Availability of a library with more than 170 questions already divided by argument, to build an assessment campaign
- Possibility to create some questions anew by the platform administrator, with text and graphic components and with true/false and multiple answers.

5.3 Characteristics of the Training modules

- Great availability of training modules specific for any subject, including some that are not specifically IT-related, but useful to address determined components to the inside and the outside of the company (see FIG.4)
- The education modules can be completed in a short time (7 to 15 minutes each), to maintain a high attention level; they can be carried out within the working hours without diverting the employees from their daily tasks.
- If an issue requires a more extensive training, it is subdivided by the producer in several modules
- Every module provides for both the training part and some static/dynamic exercise, also multiple within the same module.

FIG.4
Available training modules



- Within the platform we can find a module for the creation of fake phishing campaigns. Phishing is a very current issue, almost the totality of modern attacks perpetrated toward firms uses phishing technique to introduce the damaging code into the target. The platform is able to create some fake e-mails (which may be customizable in the appeareance and in the content), that are sent to users and contain links to corrupted sites, information requests or attachments including an harmful code. Based on users behaviour we would be able to actually assess whether the training on the topic of phishing was correctly implemented and effective.

Characteristics of Phishing campaings include:

- Presence of a great number of e-mail templates divided by subject: internal e-mail sent by ICT, security or HR, mail consumer, mail marketing, lotteries, social networks, etc.
- Possibility to send e-mails in different times to different users
- Possibility to include fake links and attachments in the e-mail which, at their opening, visualize a page (teachable moment) where is stated that is a test, and that the user should have put more attention to some particulars.
- Report where is possible to distinguish if the mail has not been opened, has been opened and cancelled, or has been opened and closed, if someone clicked on a link/ attachments, etc.

5.4 Analysis and Reporting features

- Presence of a great number of reports providing information on: assessment campaigns, training campaigns, evidence of issues highlighted as critical, comparison between assessment campaigns, users performance, risks, etc.
- Every report is composed by a graphic component with aggregated data and a tabular-like component for data in detail
- It is possible to filter data related to dataset object of the report, to have some specific information about areas and actors.
- It is possible to define and sort the columns in the tabular view.

6. CONCLUSION

Security awareness is therefore an urgent and important matter to address within the company, regardless of its type and market sector.

The return on investment is easy to demonstrate simply by referring to the decrease in IT security incidents suffered in recent years and by evaluating their direct and indirect costs. To this we must add that this goal is an integral part of many general and sector regulations.

However, we must not forget to set it as a business process that, like the others, must continue over time and evolve with the evolution of platforms and threats.

7. WHY AFKC

Despite its recent foundation in 2016, AFKC relies on a team of professionals with many years of experience in Cyber Security and Anti-Fraud

AFKC operates through offices located in Italy and The Netherlands, ensuring a consistent presence on the National and International territory.

Adding our knowledge to Kaspersky Lab's solutions, we are able to help our Partners protect End User's Business, Information and Infrastructures from Advanced Threats, Cyber Attacks and Cybercrime. We work in cooperation with our Partners (System Integrators, Solution Providers, MSPs, VARs and Resellers) offering highly specialized services and dedicated contact persons.

Our Services

SALES ENABLEMENT

PRESALES ENABLEMENT

INTEGRATED SOLUTIONS

EDUCATION

PROFESSIONAL SERVICES

TECHNICAL SUPPORT

AFKC
Value-Added Distributor

CONTACTS

AFKC B.V.

Papendorpseweg 100
3528 BJ Utrecht, Netherlands
+31 030 799 1037
info@afkc.eu

AFKC s.r.l.

Via Fiume Giallo, 3
00144 Rome, Italy
+39 06 522 44040
info@afkc.eu

WWW.AFKC.EU