Feature

The Underestimated Social Engineering Threat in IT Security Governance and Management

Roberto Puricelli, CISM, is a senior information and communications technology (ICT) security consultant at CEFRIEL, an innovation company of Politecnico di Milano. He has experience in various domains of information security, including vulnerability assessment, penetration testing, web application and mobile security, and risk analysis. He is involved in research on new generation threats, with a particular focus on social engineering attacks. As such, he contributed in developing a specific methodology aimed at measuring the related risk.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

The cybercrime ecosystem is radically changing. The evolution of some key technologies and the increased availability of powerful malware enable a business-oriented mind-set among cybercriminals. In recent years, numerous cases of advanced persistent threats (APTs) and data breaches have been seen, with those involving the largest, most high-profile enterprises garnering the most media attention. These scenarios represent only the known cybercrime issues, while, most likely, many attacks have not yet been detected or disclosed to the public. From this point of view, 2014 was a critical year: Large enterprises such as Sony, JP Morgan Chase, Target and many others suffered cyberattacks with serious consequences for the companies and their customers.

From the analysis of new attack strategies, it becomes evident that, more frequently, cyberattackers are seeking to gain a foothold into a corporate network by leveraging vulnerabilities and, from there, moving laterally to extend the compromised perimeter and take control of other systems within the target company in order to gain access to critical information. Moreover, the first phase in the attack frequently involves employee behaviors manipulated through social engineering techniques.

THE HUMAN FACTOR AS A NECESSARY PART OF INFORMATION SECURITY

Historically, employees have been the source of most security issues in organizations. The first aspect is related to the insider threat, meaning any disgruntled, mischievous or deviant employee (as well as former employee, consultant or business partner) who could take advantage of information or systems' internal knowledge to damage the company. In addition to the traditional role of the insider, the oblivious employee must be considered as well and will be the focus of this article. This individual, driven by a social engineering attack, may put corporate information at risk by performing a malicious action without realizing it. Cybercriminals understand that social engineering techniques can be used to manipulate their victims to obtain sensitive information and convince them to perform certain operations, thus increasing the success rate of attacks.

Também disponível em português
www.isaca.org/currentissue

As a matter of fact, some of the most recent data breaches can be considered examples of this scenario. The ICANN data breach originated from spear phishing, which allowed attackers to gain access to users' information on the centralized zone data system.[1] According to the investigations performed on the Carabank attack, which involved several banks across different countries, employees were targeted by social engineering attacks that allowed for the delivery of malware.[2]

Research confirms that the human factor is a weak point in the IT security chain. For example, it has been demonstrated that offering a reward of US $1 is enough to convince a large percentage of users to download and run a potentially malicious software, ignoring the typical security warning.[3]

Human error or misbehavior is often related to a lack of risk perception associated with nonrational factors, such as personal experience and psychological attitude, especially in cases of poor or missing awareness. A confirmation of this fact comes from the practice of phishing, which remains one of the most effective weapons for social engineering, even in a context where cyberattacks are constantly evolving and becoming more sophisticated.[4]

For all these reasons, it is no longer possible to limit the governance and management of enterprise IT (GEIT) to technological matters only. In the past, following the best guidelines when acquiring new appliances and configuring systems was enough to maintain an adequate level of security. Data breaches and other threats were just a remote thought for enterprises.

Unfortunately, this is not the present reality. The point is not whether IT security professionals of targeted companies deployed the best technology, processes and solutions (to be fully compliant with industry practices and standards). Rather, the relevant fact is that those security measures are no longer enough. Security attacks increasingly rely on human vulnerabilities; hence, it is fundamental to extend IT security governance to include the human factor into corporate risk analysis and assessment. To do this in an effective way, it is critical to understand and measure the actual risk and to propose effective and tailored countermeasures to mitigate it.

HOW TO ASSESS THE HUMAN FACTOR

Current approaches to IT security and risk management tend to underestimate—or even ignore—the human factor in the assessment models, tools, processes and legal structure. Since involving employees inside an assessment is a relatively innovative approach and is considered risky, planning the assessment in a proper way assumes an important role. First of all, IT and security departments are not the sole actors to define the assessment, because people are the targets. Therefore, it is necessary to involve all the relevant stakeholders, such as human resources (HR), legal and communications departments, in order to explain the threats, share the objectives, define the scope of the assessment and obtain commitment. Moreover, there are several ethical concerns and requirements that need to be considered when performing an assessment on the human factor.[5]

Social engineering attacks mean that an employee is deceived into violating a policy. Despite the fact that unscrupulous cybercriminals will make these attempts, enterprises must observe serious ethical and legal limitations, in particular, guaranteeing the respect of the trust relationship between employer and employee and avoiding invasion of an employee's personal sphere. Furthermore, it is necessary to consider the labor legal frameworks, which are radically different between the US and Europe, where employees are protected from any interference from the employer. For example, in Italy, the law prohibits an employer from monitoring the behavior of employees; hence, in an assessment, it is not possible to reveal the details of single users who may be involved in an attack. Despite the limitations and the presence of some legal and ethical risk, interest in this topic is increasing, even in Europe.

Since 2010, the assessment of several large European enterprises trying to overcome the difficulties related to this kind of activity has resulted in the development of the Social-driven Vulnerability Assessment methodology.[6] The aim of this assessment is to test human behavior against a spear-phishing attack simulation, in which an attacker attempts to trick users (i.e., company personnel) into performing actions that could put company assets at risk, for example:

1. Getting the employee to click on a link inside the email, visiting a possible malicious web site and, thus, exposing the organization to a drive-by-infection attack
2. Getting the employee to insert certain requested information into a web site form, thus providing critical information such as enterprise credentials

By using a controlled web site and tracking the users' behavior, it is possible to measure the inclination of employees to fall victim to such an attack, and it is also possible to estimate the level of exposure of the enterprise to technological follow-up attacks from the simulated phishing campaign (e.g., identifying unpatched services that can be exploited through a system fingerprinting).

WHAT IS THE ACTUAL RISK?

A significant number of assessments using the Social-driven Vulnerability Assessment methodology were performed in large enterprises (more than 12,000 employees) to try to gain an understanding of (or at least to have an idea about) the level of risk.

In most of these assessments, a spear-phishing campaign that relied on generic hooks (i.e., related to general topics that may be attractive for users, such as special offers or discounts for employees) was performed. Most of the attacks were just slightly contextualized to the specific company (through colors, logos, templates and proper styles of communication). In some cases, a reference to a specific company (based on publicly available information) was used. This did not significantly influence the results.

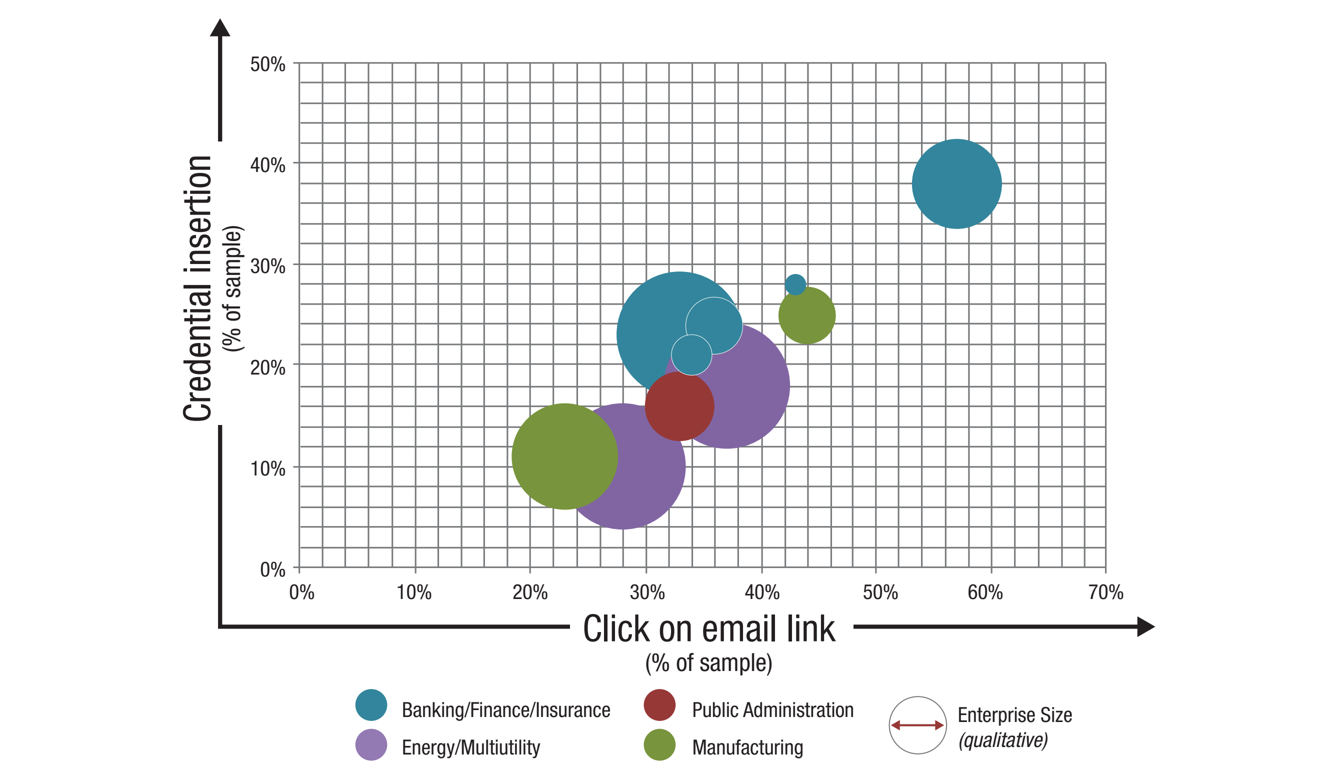
Figure 1 shows a comparison of the results of the assessments, plotting the success rate of each of the two steps described previously for the sample involved in the test: percentage of employees who clicked on a link inside the email on the x-axis and percentage of those who inserted the company credentials on the y-axis. Each circle represents an assessment performed in a company, its radius represents the size of the company itself and the color represents the industry sector. The average results are quite impressive and confirm that spear-phishing attacks actually work quite well. In these assessments, one employee out of three (34 percent) followed the link contained in a phishing email, and one out of five (21 percent) also inserted company credentials in the web site form.

These results are even more impressive when correlated to the temporal factor. According to these results, a phishing campaign is characterized by an impulsive behavior of the employee that causes a rapid growth of the success rate in the early phases, reaching a 50 percent effective rate in only 20 minutes. That means that the available time frame for an effective reaction from the information and communications technology (ICT) security function is quite short. Especially in big enterprises, there seems to be a lack of formalized processes that allow enabling countermeasures based on users' reports and, frequently, a poor level of employee knowledge with regard to how to report a security incident.

Another interesting point is that all employees are subject to this threat. There does not seem to be any particular difference when analyzing the results according to age, location, department or role. Even management and executives are often quite vulnerable. In general, it has been observed that the higher the role in the company, the lower the exposure, but the percentage of deceived managers is not marginal, posing some problems that should be considered from a risk management perspective.

Finally, through fingerprinting techniques, information was gathered on the security posture of the devices used to browse web sites (the users' workstations), and vulnerabilities were found that introduce a high level of exposure to

Figure 1—Comparison of the Results of Social-driven Vulnerability Assessments



Source: CEFRIEL. Reprinted with permission.

technological attacks. This means that using a combination of slapdash exploits, malware code and customized (yet simple) obfuscation techniques, it is possible to bypass the technological countermeasures inside a company and obtain a privileged access to the internal network, exactly the main goal of modern cyberattackers.

HOW TO MITIGATE THE RISK

From an information security governance point of view, the end goal of including the human factor into vulnerability assessment activities should be to identify suitable mitigation. The most effective countermeasures against the highlighted risk are awareness and training, which help improve the security culture of employees.

> "The end goal of including the human factor into vulnerability assessment activities should be to identify suitable mitigation."

Unfortunately, traditional awareness programs are not always effective,[7] based on the fact that some of these tests were performed just after an awareness program was put in place. No significant variations from the average results were seen in these cases. Or, at least, effectiveness of awareness programs is not usually measured.

Cybercrime enabled by social engineering is a threat that can be easily understood by nontechnical people, and having a quantitative indication of the risk could enable a better commitment and budget for corrective remediation. An objective measurement also enables the prioritization of targets for training. Furthermore, repetition of the assessment before and after training programs may help in evaluating the effectiveness of awareness programs.

The real issue is how to create long-lasting training programs that could effectively increase the security level of the company and how to then maintain this increased level of security.[8, 9] Traditional awareness programs sometimes fail because users may lack motivation to learn and to make paying attention to different signals of fake communications part of their daily habits.

Finding the right way to raise awareness is a key factor. The most promising attempts are related to using visual elements, such as video, infographics or info pills to stimulate people. Moreover, gamification is one of the most promising trends. Rewards, social engagement and direct feedback during everyday working life can help, even if the right strategy depends on different factors that must be carefully explored.

THE SOCIAL ENGINEERING RISK MANAGEMENT STRATEGY

The human factor, in particular the social engineering aspect, is a relevant vulnerability of enterprises' systems. This particular risk area is often underestimated and hard to manage. Employees may be the victims of attacks based on social engineering because they do not have the necessary training about these threats or the ability to recognize which kind of web sites or file attachments are safe to open. It is critical to conceive a strategy for including this specific human-factor-related risk in the security IT governance processes.

COBIT® 5 also considers human factors and behavior as key enablers (albeit often underestimated) for designing a holistic approach for GEIT.[10] Assessments targeting the human factor add an effective metric to measure the level of achievement of the information security goal. It is essential to establish good practices with the purpose of correcting, encouraging and maintaining the security culture throughout the enterprise. In particular, communication and security awareness and training are activities that must be performed in a proper way to increase their effectiveness.

The application of a holistic approach in this sense may be difficult. A solution should include increased internal collaboration among the stakeholders of the departments involved. This can be achieved by transferring, in a simple way with objective results and measurable figures, the perception of the actual risk to nontechnological functions, such as the communications or HR departments. This collaboration may also be valuable to redefine investment planning to contrast the highlighted risk and introduce shared budgets (not just from IT) on human-factor, security-related activities, because the actions shift from the technological to the HR field.

Collaboration among departments can support enterprises and help them to define and implement programs that effectively allow for improving the governance of information security.

CONCLUSION

Nowadays, it is not possible to reach an adequate ICT security level with only technological countermeasures, because modern cyberattacks could bypass all the defense layers, exploiting the human factor through social engineering techniques. The results discussed in this article confirm the fact that employees can be deceived to perform dangerous actions that may put the company at risk. Hence, in order to mitigate this risk, companies must develop a strategy aimed at understanding the actual extent of the problem and promoting effective actions.

> "Companies must develop a strategy aimed at understanding the actual extent of the problem and promoting effective actions."

To identify the actual level of risk, the claim that companies need to assess their employees is spreading. Due to the criticality of this step, from both ethical and normative perspectives, companies must rely on a specific and tailored methodology that can measure the potential effectiveness of a social engineering attack. Effectively applying such a specific methodology, the achieved results have proved to be useful to obtain commitment from senior management in order to implement mitigation actions, mainly related to employees' education.

In fact, to raise awareness in order to mitigate the risk, potential investments should not be focused only toward traditional education but also toward experimentation of innovative ways of awareness. This could be quite useful in effectively changing the company culture and contributing to elevation of its overall security level.

ENDNOTES

[1] ICANN, "ICANN Targeted in Spear Phishing Attack. Enhanced Security Measures Implemented,"16 December 2014, *https://www.icann.org/news/announcement-2-2014-12-16-en*

[2] Kaspersky Lab, "The Great Bank Robbery: The Carbanak," Securelist, 16 February 2015, APT, *http://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/*

[3] Guanotronic, "It's All About The Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice," *http://guanotronic.com/~serge/papers/fc11.pdf*

[4] Dhamija, R.; *et al.*; "Why Phishing Works," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2006, *www.cs.berkeley.edu/~tygar/papers/Phishing/why_phishing_works.pdf*

[5] Mouton, F.; *et al.*; "Social Engineering From a Normative Ethics Perspective," *Information Security for South Africa (ISSA)*, Johannesburg, South Africa, 2013, *http://icsa.cs.up.ac.za/issa/2013/Proceedings/Full/77/77_Paper.pdf*

[6] Brenna, R.; *et al.*; CEFRIEL, "Social Driven Vulnerability," *Technology*, February 2014, *www.slideshare.net/CEFRIEL/social-driven-vulnerability-english-version*

[7] Kumaraguru, P; *et al.*; "Teaching Johnny Not to Fall for Phish," Journal ACM Transactions on Internet Technology, 2010

[8] Kumaraguru, P.: *et al.*; "Lessons From a Real World Evaluation of Anti-phishing Training," APWG eCrime Researcher's Summit, January 2008

[9] Caputo, D.; *et al.*; "Going Spear Phishing: Exploring Embedded Training and Awareness," *Security and Privacy*, IEEE, vol. 12, iss. 1, 23 August 2013

[10] ISACA, COBIT® 5, USA, 2012, *www.isaca.org/cobit*