TOWARDS INFORMATION SECURITY AWARENESS

Prof. Marius PETRESCU, PhD, Prof. Delia Mioara POPESCU, PhD, Nicoleta SÎRBU, PhD St.
Valahia University, Târgoviste, Romania

ABSTRACT

Information security has come to be recognized as increasingly important because global communication and information systems allow a potentially large number of unauthorized users to access and possibly alter information from around the world. As the dependence on information systems grows, so the security of information networks becomes ever more critical to any entity, no matter if it is a company or a public institution.

Information security involves both technology and people. Any security system, no matter how well designed and implemented, will have to rely on people. The fact is that users, broadly defined to include both end-users and system administrators, play a key role in implementing and correctly operating and maintaining security controls. At the same time, statistics reveal that a large number of security incidents are caused by users failing to comply with security controls. There is no use to implement complex and expensive technical solutions, if measures are not taken to deal with users security awareness rising.

This paper aims to draw attention over the key role of the users in ensuring the information security and the need to develop coherent information security awareness programs, as part of the information security management process in any organization.

The study is based on statistics analysis regarding information security incidents and consequent losses caused by users and the results obtained by implementing specific awareness programs.

Keywords: security awareness, security controls, information security

JEL Classification: D81, L86

Paper type: Conceptual paper

Introduction

Computer crimes are on the rise, and the damage they produce is becoming more severe. Large servers, desktop computers, laptops, printers, hand-held PDA's, and other devices are all targets for attackers.

Recent high-profile data breaches have raised concerns, leading private and public organizations to understand that policies and technologies must be put in place to secure sensitive organization information [ENISA, 2009]. These controls have to ensure the ability to secure information on the network as well as the opportunity to manage data going in and out of the company. While policies and technology are certainly a critical part of any information security program, these measures alone cannot deliver sufficient information security in practice.

Awareness of the related risks and available safeguards is the major line of defense for security. Employees are the real perimeter of the organization's network and their behavior is a vital aspect of the total security picture. Protecting organizations begins with making sure employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources and assist the organization in keeping computers and network safe.

In the modern multi-user computer environment, Internet-capable network servers provide connectivity that allows a large portion of the user population to access information at the desktop from sources around the world. Because of the ease with which information can be accessed, computer security breaches may occur unless systems and restricted information stored therein are kept secure [Schultz E. E. et al., 2001]. Breaches of security can have serious consequences, including theft of confidential corporate documents, compromise of intellectual property, unauthorized modification of systems and data, denial of service, and others.

Numerous sophisticated security methods have been developed, many of which rely on individuals to implement and use them. However, these methods may not accomplish their intended objectives if they are not used properly. Simple human error, ignorance or omission is most commonly at the root of any security breach.

Many successful attackers today simply take the easy road; they exploit well-known vulnerabilities, using the tools handed to them. By taking a few simple steps, security-aware computer users can foil these attempts. Raising awareness will improve security far more effectively than any technical solution can ever hope to achieve [Hadfield R., 2009].

Information security

Information security is one of the important components of the security system for any organization and for this reason it must be considered an integral part of an organization management system. Information security is done using the main management mechanism for the organization's security and should consist of protecting both the inside information flow and the communication with outside entities in order to guarantee that the organization can reach its mission.

Information security rests on confidentiality, integrity, and availability of the information and on integrity and availability of the services and resources of the communication and information systems throughout which information are handled.

From a realistic point of view, security has always been about mitigating risk; surviving the panoply of threats our world throws at us [Andress A., 2003]. Information security in its most basic sense is protecting computer-related assets such as computers, networks, data, programs, and the hardware components.

The need for security has existed since the introduction of the first computer. The paradigm has shifted in recent years, though, from terminal server mainframe systems, to client/server systems, to the widely distributed Internet [Andress A., 2003]. Although security is important, it has not always been critical to an organization's success. With a mainframe system, organizations had to take care to mainly protecting their systems from resource abuse-either authorized users hogging resources or unauthorized users gaining access and using spare resources. Such abuse was damaging because system resources were costly in the early days of mainframes. As technology developed and the cost of system resources decreased, this issue became less important. Remote access to systems outside an organization's network was almost nonexistent. Additionally, only a limited community had the knowledge and tools necessary to compromise a mainframe system.

The development of client/server technology, however, led to numerous new security problems. Processor utilization was not a priority, but access to networks, systems, and files grew in importance. Access control became a priority as sensitive information was being stored on public file servers. Organizations did not want this type of data to be public knowledge, even to their employees, so new technologies such as granular access control, single sign-on, and data encryption were developed. As always, methods of circumventing and exploiting these new applications and security products quickly arose.

Every level of threats implies the design and implementation of adequate countermeasures, meant to eliminate or to diminish the possibility for the identified threats to exploit systems' inerrant vulnerabilities.

"Information security controls" (also called "information security mechanisms") are techniques and procedures used to reduce the likelihood that security related threats will result in unauthorized disclosure or possession of information, loss of integrity of systems and/or data, and disruption of availability and/or accessibility of systems [Schultz Eugene E. et al., 2001]. Nowadays there are numerous sophisticated security control mechanisms, examples of which are passwords used to log on to systems, file permissions and cryptographic devices. On the other hand, technical mechanisms are often backed by non-technical mechanisms such as requiring proof of identity before changing a password. In fact, policies often require some procedural mechanisms that technology cannot enforce.

However, there are factors that can significantly influence the implementation of and compliance with security controls. E.g. throughput pressure, by imposing higher priority on production and less on security; cost-benefit factors, incl. perception of personal gains and losses; conflicts between personal and organizational goals – both acting to the detriment of security goals; and finally risk, or rather perceived risk [Gonzalez J. J. and Sawicka A., 2002]. All these determine a user resistance towards systems with which they must interact [Schultz E. E. etl. al., 2001]. The inertia is more pronounced when users are not aware of the potential negative impacts that a threat can have over the mission of their organization and, ultimately over their personal interests. Since many (if not most) security-related controls rely on individuals to implement and deploy them, more attention should be given to developing awareness and learning programs, targeting the specific categories of users, including system and security administrators.

Unfortunately, although companies spend considerable sums on up-to-date security technology, they often ignore the other two components: people and process. Like a three-legged stool, a security infrastructure needs all three supports to maintain balance and effectiveness [Andress A., 2003].

This paper aims to draw another alarm signal over the need to design, implement and maintain a balanced set of procedural and technical controls in order to achieve the objectives of information security. The focus is put on developing and applying awareness and learning programs, since we consider this "stool leg" is less developed and may represent a major vulnerability of the security system.

Information security awareness

Users have long been regarded as the weak link in information security. That is why information security awareness and training should be one of the most critical aspects of any organization's information security strategy and supporting security operations [Microsoft, 2010]. This is due to the realization that people are in many cases the last line of defense against threats such as malicious code, disgruntled employees, and malicious third parties.

Therefore, people need to be educated on what your organization considers appropriate security-conscious behavior, and also what security best practices they need to incorporate in their daily business activities.

Security awareness is the human knowledge and behaviors that the organization uses to protect itself against information security risks. People, just like computers, store, process and transfer information. As a result many attackers today target the human, bypassing most security controls and using techniques such as social engineering to get the information they want. Awareness, not just technology, is now a key factor in an organization's goal to reduce risk, protect its reputation, improve governance, and be compliant.

Recent cyber events have raised concerns, leading private and public organizations to understand that while policies and technology are certainly a critical part of any information security program, these measures alone cannot deliver sufficient information security in practice. Awareness of the related risks and available safeguards is the first line of defiance for security. People are the real perimeter of the network and their behavior is a vital aspect of the total security picture.

What do statistics reveal?

Although there are a lot of analyses concerning the budget spent by different organizations for implementing technical security controls, only a few of them are approaching the security awareness issue.

The 2008 CSI Computer crime and security survey [CSI, 2008] was the fist to raise the question regarding the percentage of the security budget allocated for awareness training. The answers to this question were somewhat surprising, since they reveal very low expenditures allocated to security awareness, as a percentage of the total security budget of the questioned organizations. Some 42% of the questioned organizations spend less than 1%of their security budget on awareness programs, 19 percent spent between 1 and 2%, 12%spent between 3 and 5%, 3% between 6-7%, while only 5% between 8-10% on awareness programs. This survey reveals that there are relatively small budgets allocated to information security awareness, compared with budgets allocated to other security mechanisms and programs. The 2008 CSI Survey concludes that it's difficult to say why these numbers are lower than some of the discussions around the importance of security awareness training might suggest. On the one hand, many forms of security awareness training can be delivered at a relatively low cost. Additionally, one of the principal costs of any sort of training — the time that employees spend away from productive work in order to take the training — is borne outside the security budget. But low training expenditures may also reflect a general cynicism about the necessity or effectiveness of awareness training.

The statistics show, however, that the general level of awareness is rising, and the focus now needs to be on changing and measuring actual behavior. The 2008 Information Security Breaches Survey [Price WaterHouse Coopers, 2008] reveals that, if in 2004 only 40% of the respondent organizations stated that they provide ongoing security awareness training to staff, in 2008 the percentage was of 80% of the respondent organizations.

In 2010 Price WaterHpuse Coopers conducted an analysis [Price WaterHouse Coopers, 2010] regarding information security practices from the perspective of different countries around the world. Not surprisingly, taking into consideration its late development and IT/C potential, China emerged as a leader in global information security practices. When coming to information security awareness issues, organizations stating they developed an employee security awareness program represented 59% of the respondent organizations in India, 64% in

the U.S., 48% in the U.K., 36% in Germany, 48% in Brazil, 59% in Australia and 61% in China.

Thus, from 2004 onwards statistics reveal a growing trend towards giving more attention to the awareness side of security controls. This tendency was also fed by repeated security incidents that have as primarily cause the poor understanding of the responsibilities users have in ensuring security of the information they handle.

Statistics regarding information security incidents reveal that most of these are occurring due to inadequate use of information systems services and resources. According to statistics [CSI, 2008], in 2008, virus incidents occurred most frequently, occurring at almost half (49%) of the respondent organizations. Inside abuse of the network was second most frequently occurring incident (44%), followed by theft of laptops and other mobile devices (42%).

All these types of incidents reveal a poor information security culture and the need to develop information security awareness within organizations. The human factor awareness is most of the times more important than spending money on sophisticated equipments. If the attack comes from inside the organization, its probability to be successful is of around 95% [Stanciu Florentin, 2006].

Developing an information security awareness program

Since most analyst reports claim that the human component of any information security framework is the weakest link, then only a significant change in user perception or organizational culture can really reduce the number of information security breaches.

Consequently, a high personal awareness of the risks and available safeguards is recognized as a major component of the security of information systems and networks. In this, all actors, the industry and stakeholders, as well as end-users as individuals, must assume a share of responsibility.

When developing a strategy to increase the level of information security awareness, subject matter expertise, and the ability to apply principles and concepts to common business activities among your organization's workforce, it is critical to understand the two tenets of learning: awareness and training [Microsoft, 2010].

The information security learning process begins with establishing awareness. The primary objective of establishing information security awareness is to change workforce behavior by reinforcing acceptable security business practices [Microsoft, 2010]. This objective is achieved by imparting an understanding of information security considerations and enabling individuals to apply them accordingly in all settings.

A role-based information security training process follows the completion of the information security awareness process since the skills that are acquired during information security training are built upon the information security awareness foundation. The primary objective of role-based information security training is to impart relevant and necessary information security skills and competencies to practitioners, regardless of whether their professional responsibilities may involve information security. The most significant distinction between information security training and awareness is that training focuses on teaching skills, which enable practitioners to perform specific functions, while awareness directs a practitioner's attention on a particular issue or series of issues.

The information security learning life cycle is an ongoing process for two primary reasons. The first reason is that information security threats continue to evolve. In order to effectively react to evolving threats, new technologies and operating procedures are developed, requiring ongoing information security learning practices. New information security considerations and

subject matter will continue to appear, requiring an ongoing learning process. Also, it is impractical to expect practitioners to consume and absorb all aspects of information security within a concentrated amount of time.

Organizations practice various forms of awareness and training programs, in order to target the right staff. Balanced awareness and training programs, employing combined mechanisms prove to be more efficient than those programs developed on a single knowledge delivery mechanism.

What we would like to underline is that the target audience of the information security awareness programs should be not only the users and the administrators of the systems, but also the decision-makers. It is important to that the decision making process to be grounded on a solid knowledge of the threats and vulnerabilities that can have adverse effects of the organization's information, systems and, ultimately, on organization's mission.

Efficiency of information security programs

Implementing security measures is one thing; verifying that they are properly in place and effective on an ongoing basis is another.

The 2008 CSI Computer Crime and Security Survey illustrates that internal security audits are the predominant approach (47%), but also that automated tools now play a significant role, with 55 percent of respondents reporting their use. E-mail and Web monitoring are in place at half of respondent organizations (49% for each of them), as is the use of external audits (also 49%).

As regarding the effectiveness of their security awareness training programs, in order to gauge it, organizations developed diverse techniques [CSI, 2008]. The same CSI survey reveals that 18 percent of respondents don't use awareness training, implying that 4 out of 5 respondent organizations do in fact engage in training their employees about security risks and appropriate handling of sensitive data. Although a strong majority performs this kind of training, many of the respondent organizations (32 percent) make no effort to measure the effect of this training on the organization. For those organizations that made an analysis regarding the effectiveness of the training and awareness programs, the most frequent used techniques were the analysis of the volume and type of incidents, volume and type of help desk issues, social engineering testing, written / digital tests.

The evaluation of the results of an awareness and training program is important from at least two perspectives. First, it is the program's objective itself. If the program does not achieve its objective of enlarging the user's knowledge regarding the threats and vulnerabilities that can affect information handled within their organization, the mission of the organization may be at risk. Second perspective is that the awareness and training program must be developed and improved in accordance with the organization's needs and target audience. A lack of effectiveness should trigger an improvement process of the program. Feed-back on the program should always be required from both the participants to the program and the managers that have responsibilities over the information systems within the organization.

EU efforts towards information security awareness

Recognizing the importance of information security within the modern society, at the level of the European Union it was established the European Network and Information Security Agency (ENISA). ENISA is an EU Agency established to advance the functioning of the internal market.

ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the Agency facilitates contacts between the European institutions, Member States and private business and industry actors.

To this end, ENISA is engaged in positively influencing public behavior towards information security, changing the mindset of the human element in order to achieve greater information security awareness.

During 2007, following the positive feedback received and the common willingness to create a recognized and established Information Security Awareness Community, ENISA included in the framework of the multi-thematic annual program of the Agency ('Developing and maintaining cooperation models') the creation of the Awareness Raising (AR) Community [ENISA, 2010].

Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Ireland, Italy, Malta, the Netherlands, Norway, Portugal, Romania, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United Sates, Cyprus and Vietnam joined in February 2008, followed by Egypt, Luxembourg, Morocco, New Zealand in April 2008, Australia and Latvia in May 2008, Lithuania and Poland in June 2008 and Bulgaria, Czech Republic and Sierra Leone in July 2008. The growth of the community steadily continued in the second half of 2008 by having people from FYROM, Israel and Lichtenstein as new members. From January to May 2009, the AR Community grew by 60% and got its first members from China, Canada, Malaysia and Mexico.

Most of the AR Community's population growth is due to a common recognition of the importance of information security awareness.

The AR Community objective is to raise information security awareness within their organizations regardless of the sector to which they belong. The main mechanisms developed by the AR Community in order to achieve its objectives are the organization of thematic meetings, the publishing of awareness materials, bulletins and reports, ensuring a permanent dialog between its members and being a link between public and private sector on issues regarding information security.

Conclusions

Organizations increasingly realize that their people, while their greatest asset that make them function on a day-to-day basis, can be their greatest vulnerability, and so need to be educated on security risks.

Developing a security awareness program is essential for any organization that seeks to reduce the risk of data loss and theft, assure that information assets are appropriately secured, and meet various regulatory requirements. After a period when technical controls played the major role in the information security puzzle, risk assessments revealed the necessity to embed security awareness more deeply across the organizations. Perhaps the most powerful driver of positive security outcomes is awareness.

The current challenge of information security is to change the culture of information systems users to a more information security conscious one. Starting from the level of international organizations, government institutions and private organizations, all have to cooperate in achieving a sound security culture for those using communication and information systems. Being aware that inappropriate behavior when using communication and information systems may put at risk the organization's, as well as personal, interests is the starting point towards implementing effective information security systems.

Though most of the times less expensive than technical security controls, information security awareness has a more positive impact over the overall security posture of an organization. The development and implementation of an awareness and training program addressed to all users with access to the information system is one of the pieces without which the information security puzzle would be incomplete and, though, inefficient.

References

Andress Amanda (2003), Surviving Security: How to Integrate People, Process, and Technology, Auerbach Publications, Boca Raton, FL, USA

Computer Security Institute, US (CSI) (2008) CSI Computer Crime and Security Survey, available at http://i.cnpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

European Network and Information Security Agency (ENISA), (2009): The growing requirement for information security awareness, Publications Office of the European Union, Luxembourg

European Network and Information Security Agency (ENISA) (2010) Key facts and figures about the AR Community and its members, Awareness Raising Community

Gonzalez Jose J, Sawicka Agata (2002), A Framework for Human Factors in Information Security, 2002 WSEAS Int. Conf. on Information Security, Vol.20, No.7, pp.620-634, 2001, Rio de Janeiro

Hadfield Rob (2009), CISSP, ENISA Conference, 19th June 2009

Microsoft Information Security Awareness Program, available at http://msdn.microsoft.com/en-us/security/cc165442.aspX

Price WaterHouse Coopers (2008), Information Security Breaches Survey, available at http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

Price WaterHpuse Coopers, (2010), What global executives expect of information security—in the middle of the world's worst economic downturn in thirty years, available at http://www.pwc.com/gx/en/information-security-survey

Schultz E. Eugene, Robert W. Proctor, Mei-Ching Lien, Gavriel Salvendy (2001), Usability and Security An Appraisal of Usability Issues in Information Security Methods, Computers & Security Vol.20, No.7, pp.620-634

Stanciu Florentin (2006), Market Watch, no. 90, November 2006