THE ROLE OF INFORMATION SECURITY AWARENESS FOR SENIOR EXECUTIVES

Sandor Magyar | 0000-0002-6085-0598 | magyar.sandor@uni-nke.hu
Ludovika University of Public Service, Military National Security Department, Budapest, Hungary,
Andras Tóth | 0000-0001-6098-3262 | toth.hir.andras@uni-nke.hu
Ludovika University of Public Service, Signal Department, Budapest, Hungary,
Peter Banyasz | 0000-0002-7308-9304 | banyasz.peter@uni-nke.hu
Ludovika University of Public Service, Cyber Security Department, Budapest, Hungary,

Abstract

Supporting services in cyberspace plays an increasingly important role in our daily lives. This is not just in our private lives, but also in various areas of business, government, and administration. The rapid development of electronic information systems is making us more efficient, but our growing competence is also making us more dependent on IT services. The infiltration of IT services into our business processes is also triggering the development of cybercrime. The number and the complexity of cyber-attacks in cyberspace are increasing, and the damage caused by cybercriminals is growing therefore the need to defend against attacks from cyberspace is urgent. There are several possible areas of defence, one of them relating to information security awareness. In addition to the importance of awareness raising, this publication focuses on awareness raising among senior executives. Senior executives in organisations can be the focus of targeted cyber-attacks much earlier, because they have a higher level of authorisation, access to more systems, more sensitive information in their e-mail correspondence, etc. The role of senior executive awareness is therefore indispensable to reduce the risks. However, as managers' time is limited, it is necessary to find the right theme and timeframe for awareness-raising. The threats they face, and how to protect themselves against them must be communicated in the language they can understand. Also, in addition to explaining the impact of threats, the results of risk analyses should be used to effectively communicate protective measures and the dangers of residual risks.

Keywords: Awareness, Cyber Security, Cyberspace, Information security, Resilience

Introduction

In our accelerating world, IT systems support is becoming indispensable. Electronic information systems are making more and more areas of life easier, systems that play a major role in increasing efficiency and effectiveness, in addition to providing convenience services. The COVID-19 pandemic has boosted the development of digitalisation and the need for teleworking. Along with teleworking, the number of remote accesses has also increased, with users accessing systems in bulk from off-site. The development of technical systems is necessary to meet these demands, and the implementation of protection measures is inevitable, but there is one factor that also plays a major role in cyber security and that is the human factor.

The role of the human factor in security is becoming increasingly important. According to the Verizon 2023 Data Breach Investigations Report (DBIR) (Verizon DBIR, 2023), "74% of all breaches involve the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering." The human element can influence security in a number of ways, one of which is intentional compromise, which is not addressed in this article. In addition, a lack of training or awareness of information security, as well as a lack of conscious behaviour, can also be a significant risk.

Research has confirmed that security-aware CEOs and managing directors are more convinced that IS security brings a firm's advantage. Contrary to this, business executives who are not aware of the importance of their firm's IS security, are more likely to appraise security as unnecessary or less important. (Olt, Christian; Gerlach, Jin, 2019).[1]

Challenges of information security awareness

The number and the complexity of cyber-attacks in cyberspace are increasing, and the damage caused by cybercriminals is growing therefore the need to defend against attacks from cyberspace is urgent.

There is a growing knowledge gap between the people who carry out cyber attacks and the average user. A higher percentage of internet users are not keeping up with threats from cyberspace.[2] (Légárd, 2021)

We are facing a number of threats that were not present in such quantities before. One of today's challenges is to keep pace with the development of technology. Understanding emerging and disruptive technologies such as artificial intelligence, quantum computing, autonomous vehicles, etc., requires technical knowledge alone, but in many cases, the use of these technologies requires training and awareness. These technologies can greatly support development, but they can also be used for the wrong purposes.

Information security challenges in supply chains are becoming increasingly important. They are also a major concern for cyber security in the context of business continuity.

The opportunities for Open Source Intelligence (OSINT) have increased with the penetration of the Internet. In many cases, publicly available information provides an opportunity to prepare for cyber-attacks. OSINT

[1] Olt, Christian; Gerlach, Jin; Sonnenschein, Rabea; and Buxmann, Peter, "On the Benefits of Senior Executives' Information Security Awareness" (2019). ICIS 2019 Proceedings. 25.
https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/25

[2] Legárd, Ildikó, Játék a jövőért: Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével, POLGÁRI SZEMLE: GAZDASÁGI ÉS TÁRSADALMI FOLYÓIRAT 17 : 1-3 pp. 358-373., 16 p. (2021)

activities are made easier by more effective software. For this reason, being on the Internet now requires much more thoughtful behaviour than before.

The spread and impact of fake news is also growing. News in cyberspace can influence our perception of reality, which can have an impact on our decisions. Artificial intelligence can also help to generate this information and target people more effectively. Awareness in sharing these also means a kind of understanding.

Information security awareness

The location of the awareness raising is within the PreDeCo[1] principle of prevention. It allows for one of the most cost-effective solutions to defend against cyber-attacks.

„Information Security Awareness (ISA) is a knowledge and attitude of interested parties of an organization on the protection of information assets owned or managed by the organization”[2] (Tarján, 2020).

Senior executives do not usually have a background in IT, but in law or economics, for example. They are not always sensitive to the subject and do not understand IT and information security terminology. Sometimes there is an over-reliance on technology or the opposite, with a predominance of scepticism.

Without a sufficient understanding of the risks, managers are unable to make decisions on what investments, training, and awareness campaigns are needed to ensure that the IT system is protected in a way that is commensurate with the risks. If business processes are the only focus and not enough effort is put into protection measures, the chances of cyber-attacks succeeding will be higher for the organisation.

Social engineering techniques are also being developed, the understanding of which will reduce risks. One effective way to increase an organisation's security awareness is through a social engineering audit. These audits can provide a good picture of the organisation's information security awareness on which to build awareness training and campaigns.

When raising awareness of information security, it is important to consider the level of maturity illustrated in Figure 1. The level of maturity can depend on a number of factors, but senior executive expectations and support can facilitate changes between levels.

[1] Prevention, Detection, and Correction

[2] Tarján Gábor: Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben, Doktori Értekezés, Budapesti Corvinus Egyetem, 2020.

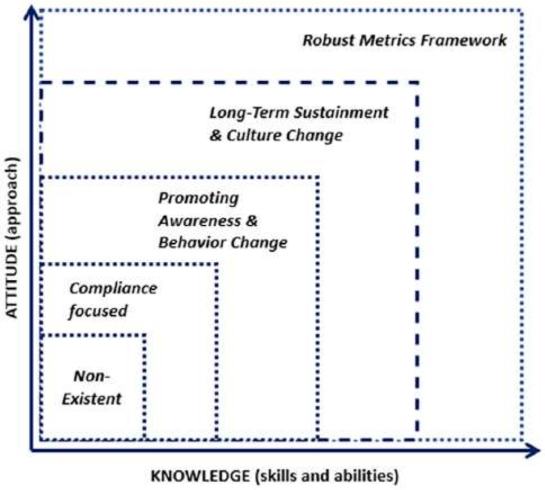
Robust Metrics Framework
Long-Term Sustainment & Culture Change
Promoting Awareness & Behavior Change
Compliance focused
Non-Existent
ATTITUDE (approach)
KNOWLEDGE (skills and abilities)

Figure 1. The role of knowledge and attitude for information security awareness maturity[1] (Kő, Tarján, Mitev, 2023)

Characteristics of senior executive's awareness

Information security awareness cannot be treated uniformly across different groups. Users of IT systems need to follow a different awareness-raising agenda than, for example, privileged users. Also, a specific targeted theme is needed for senior executives.

There are a number of differences between normal users and senior executives, which indicate that managers should receive specific targeted training:

Users	Senior Executives
Low-level authorization	Higher level of authorisation
Access to few systems	Access to more systems
Limited permission to systems	Higher permissions to systems
Less sensitive information in their e-mail correspondence	More sensitive information in their e-mail correspondence
Users are able to see fewer folders	Executives are able to see more folders
Less influence	More influence
Lower target	Main target
Reputation risk lower	Reputation risk higher

On the other hand, in addition to the above, there are other individual characteristics that influence the implementation of awareness-raising that need to be taken into account. Among other factors, age and related generational differences, education, professional qualifications, position in the organisational hierarchy, and

[1] Kő Andrea, Tarján Gábor, Mitev Ariel, Information security awareness maturity: conceptual and practical aspects in Hungarian organizations, INFORMATION TECHNOLOGY AND PEOPLE 36 : 8 pp. 174-195., 22 p. (2023)

experience of previous information security incidents may influence the implementation of awareness raising. However, a more complex approach to the issue is the Multiple Perspectives Concept (MPC) perspectives, which divides it into Technical (T), Organizational/Societal (O) and Personal/Individual factors.[1] (Linstone, 1989)

A summary of the factors adapted from MPC is shown in Figure 2. (Munir, Molok, Talib, 2017)

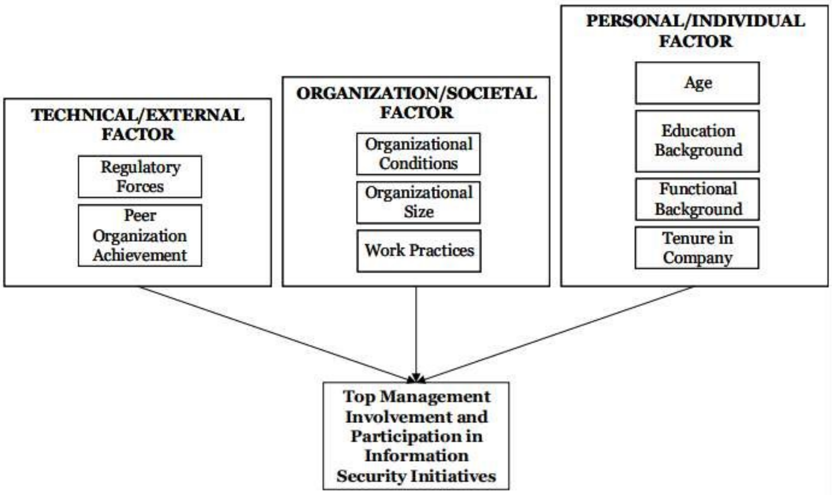
TECHNICAL/EXTERNAL FACTOR
Regulatory Forces
Peer Organization Achievement
ORGANIZATION/SOCIETAL FACTOR
Organizational Conditions
Organizational Size
Work Practices
PERSONAL/INDIVIDUAL FACTOR
Age
Education Background
Functional Background
Tenure in Company
Top Management Involvement and Participation in Information Security Initiatives

Figure 2. The Conceptual Model (Munir, Molok, Talib, 2017)[2]

An important area of managerial attitude is to allow subordinates to participate in security awareness programmes, because subordinates will appreciate the importance of security or its relevance to their tasks. [3]

It is also necessary to highlight that mistakes made by senior managers also increase the reputational risk of the organisation, as in many cases they identify the organisation or the organisational unit with the person of the executive. Awareness-raising among executives is therefore of vital importance.

It is essential to take protective measures against risks, and therefore awareness raising is based on the results of risk analyses. This can lead, for example, to a greater focus on endpoint protection.

[1] Linstone, H. A. 1989. "Multiple Perspectives: Concept, Applications, and User Guidelines," Systems Practice (2:3), pp. 307–331.

[2] Munir, Rufizah Abdul; Abdul Molok, Nurul Nuha; and Talib, Shuhaili, "Exploring the Factors influencing Top Management Involvement and Participation in Information Security" (2017).

[3] Maeyer, D.D. (2007). Setting up an effective information security awareness programme. In ISSE/SECURE 2007 Securing Electronic Business Processes (pp. 49-58)

Awareness-raising among senior executives requires implementation in small groups, possibly individually, as more attention needs to be paid to the executives and their questions during the awareness-raising should be answered in any case, thus modifying the possible topics.

Due to the workload of managers, the dates and timing of the information security awareness sessions should be agreed in advance.

Awareness also includes, for example, the understanding that no admin rights for executives. It is not possible to read other people's emails without violating their privacy, and admin rights require a high level of IT skills.

The most important goal of information security awareness raising is to understand awareness, where the objective is not to pass the exam but to understand the impact of cyber threats on the individual or organisation.

The influence of senior managers on the development of organisations is much greater, so the methodology of information security cost benefit analysis can also be of help. The management must provide a commitment to information security through its activities and budget.[1] (Johnson, 2006) Cyber security systems are high cost and have no direct impact on production or productivity. As long as attacks from cyberspace are not coming, they can be perceived as an unnecessary expense for the expensive hardware and software elements of IT systems, which also have significant annual maintenance and licensing fees. Expenditure may also be incurred by the organisation in employing the right number and skills of IT, IT security professionals, running security operations centres depending on the size of the organisation, etc. Furthermore, information security awareness may also be seen as a responsible waste of resources. However, fewer attacks, ensuring the confidentiality, integrity and availability of data stored in electronic information systems is a prerequisite for ensuring business value.

In parallel with changing user habits, the various social media platforms, among others, have come to the forefront of open information gathering.[2] (Dobák I. 2019)

For senior executives, the use of privacy-enhancing technologies has an even greater role to play, which needs to be specifically addressed in the case of awareness-raising.

The role of cyber defence exercises in management awareness raising

A major cybersecurity incident affects the confidentiality, integrity and availability of an organisation's systems. In real life, after suffering a successful cyber attack, executives may need to make appropriate decisions or possibly make statements in situations that are not entirely familiar to them. Depending on the

[1] Johnson, E.C. (2006). Security Awareness: Switch to a better programme. Network Security, February, 15-18.

[2] Dobák I. (2019), OSINT - Gondolatok a kérdéskörhöz, Nemzetbiztonsági Szemle 2019/2, pp. 83-93.

severity of the incident, immediate decisions, and crisis communications may even be required at the senior management level. The exercises provide a good opportunity to practice these.

It is important that the rapid problem-oriented thinking and crisis management required in the event of cyber-attacks, which usually occur unexpectedly and suddenly lead to drastic decision-making, are developed before the subsequent acute situations.[1] (Vikman, 2022)

Regardless of their type, cyber defence exercises can have many benefits from an awareness-raising perspective. The two main categories of exercises are Discussion-based exercises (which include seminars, workshops, and tabletop exercises) and Operations-based exercises (which include drills, functional exercises, and full-scale exercises). (HSEEP, 2017)

In cyber defence, understanding the context is crucial. Cybersecurity exercises can also show the interdependencies between different areas, which senior executives can support more responsibly. In the case of full-scale exercise, it can be quickly understood what level of attacks can be suffered if the IT staff is not adequately staffed and trained, what the consequences of lack of hardening are, what detective technologies need to be used, what the task is to collect and analyse log files, how to respond appropriately to an incident, how to build effective workflows, etc. Executives can then put more emphasis on improving the weaker areas.

Conclusion

Without top managers' IT security awareness the organisation might pay a significant price when an IT security incident occurs. [2] (Sonnenschein; Loske; and Buxmann, 2017).

The information security awareness training will not only inform participants about trends in cyber-attacks, but also about how to protect themselves and the importance of the necessary protection measures in the organisation.

For senior managers, strategic thinking is there, but responding to cyberspace and the threats it poses is not always. The result of information security awareness can be to strengthen the cyber defence area built into strategies. This will have an impact on functional strategies within the corporate strategy, such as human resources strategy, IT strategy, etc.

[1] Vikman László: Az aktuális kibertér fenyegetés jogi kihívástérképe, Katonai Jogi és Hadijogi Szemle 2022/3., 91-108.

[2] Sonnenschein, Rabea; Loske, André; and Buxmann, Peter, "The Role of Top Managers' IT Security Awareness in Organizational IT Security Management" (2017). ICIS 2017 Proceedings. 13. https://aisel.aisnet.org/icis2017/Security/Presentations/13

Bibliography / References

- Dobák I. (2019), OSINT - Gondolatok a kérdéskörhöz, Nemzetbiztonsági Szemle 2019/2, pp. 83-93.
- Johnson, E.C. (2006). Security Awareness: Switch to a better programme. Network Security, February, 15-18.
- Legárd, Ildikó (2021), Játék a jövőért: Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével, POLGÁRI SZEMLE: GAZDASÁGI ÉS TÁRSADALMI FOLYÓIRAT 17 : 1-3 pp. 358-373., 16 p. (2021)
- Linstone, H. A. 1989. "Multiple Perspectives: Concept, Applications, and User Guidelines," Systems Practice (2:3), pp. 307–331.
- Kő Andrea, Tarján Gábor, Mitev Ariel (2023), Information security awareness maturity: conceptual and practical aspects in Hungarian organizations, INFORMATION TECHNOLOGY AND PEOPLE 36 : 8 pp. 174-195., 22 p. (2023)
- Maeyer, D.D. (2007). Setting up an effective information security awareness programme. In ISSE/SECURE 2007 Securing Electronic Business Processes (pp. 49-58).
- Munir, Rufizah Abdul; Abdul Molok, Nurul Nuha; and Talib, Shuhaili, "Exploring the Factors influencing Top Management Involvement and Participation in Information Security" (2017).
- Olt, Christian; Gerlach, Jin; Sonnenschein, Rabea; and Buxmann, Peter (2019), "On the Benefits of Senior Executives’ Information Security Awareness" (2019). ICIS 2019 Proceedings. 25. https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/25
- SANS Top Ten Security Awareness Topics – Roundup, https://www.sans.org/blog/top-ten-security-awareness-topics-roundup/
- Sonnenschein, Rabea; Loske, André; and Buxmann, Peter, "The Role of Top Managers’ IT Security Awareness in Organizational IT Security Management" (2017). ICIS 2017 Proceedings. 13. https://aisel.aisnet.org/icis2017/Security/Presentations/13
- Tarján (2023): Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben, Doktori Értekezés, Budapesti Corvinus Egyetem, 2020.
- Verizon 2023 Data Breach Investigations Report (DBIR) https://www.verizon.com/business/resources/reports/dbir/
- Vikman László: Az aktuális kibertér fenyegetés jogi kihívástérképe, Katonai Jogi és Hadijogi Szemle 2022/3., 91-108.