Sándor Magyar – Imre Dobák

The Importance of Security Awareness Thinking in Cyberspace

Abstract

The ITC environment that pervades our daily lives in cyberspace is increasingly confronted with cybersecurity concerns. While our devices and services make our lives better and more efficient, their use can also carry a number of risks. Think of the growing number of cyberattacks of all kinds, or even the rise of cybercrime. At the same time, trust in cyberspace services in the developed world of the 21st century, and their credible and proper functioning, requires the necessary security conditions to be in place. This is true not only in our private lives, but also in various areas of business, government and public administration. All of these require specific defensive elements which, in addition to the technical side, also include the task of reducing vulnerabilities on the human side. In this respect, raising the level of security awareness and research into effective methods will play an important role. The paper accompanying the presentation on this topic deals with this complex aspect.

Keywords: cyberspace, awareness, security

Introduction

Cyberspace is playing an increasingly important role in our daily lives. Our comfort and efficiency are supported by IT services not only in our private lives, but also in our working environment. The evolution that electronic information systems have undergone over the last decade has brought us both great opportunities and very

DOI: https://doi.org/10.36250/01260_14

serious threats. In our changing world, the benefits of the digital ecosystem are drawing the attention of criminals to cyberspace. In parallel, the number and complexity of cyberattacks in virtual space are growing, as is the damage caused by cybercriminals. The effects of cyberattacks, whether it is the theft of data or the rendering of systems inaccessible, are all causing increasing damage to both civil society and public and governmental sectors.

Emerging and disruptive technologies, such as quantum computing, artificial intelligence, the proliferation of autonomous transport vehicles, can be both for and against security. In response, the risks that emerge with the development of these technologies will also require larger-scale security mechanisms. Just think of the challenges posed by the rapidly developing field of artificial intelligence, and in particular the ethical and moral issues raised by autonomous devices and robots. The issues of networking and interdependence also underpin the topicality of the subject, and attacks on supply chains also require greater attention from the defence side.

Prevention, detection and remediation are the triple bottom line for categorising cybersecurity activities. Prevention seems to be the easiest area to defend against attacks, but the cost of the effort is not always commensurate with the risk. This brings to the fore a complex approach, including the importance of human awareness.

Attitude

But what can be built on to increase the security awareness of individuals? Security-aware behaviour should fundamentally rely on intrinsic motivation, increasing security and understanding the impact of cybersecurity incidents. Timely identification and avoidance of risks is crucial. Awareness-raising should focus not only on learning processes but also on cognitive achievements that can help to understand the impact of negative processes after damage has occurred.

A detrimental approach can be to reinforce the fear of punishment, since, while in many cases "by the book" behaviour and maximum security compliance cannot be bagatelles, fear of punishment can help to keep a significant proportion of cybersecurity incidents in the background (increasing latency). As a result, the impact of cybersecurity incidents is often only faced when the real, often irreversible, damage occurs. The issue of cybersecurity incidents and latency is in itself a wide-ranging area worthy of research, which can be attributed to a variety of causes, whether due to lack of information or human characteristics. Among these, the present study highlights cases where:

- The attacked person does not notice the cybersecurity incident.
- Notices the cybersecurity incident, but fails to appreciate or dismiss its significance (the reasons for this may be due to either personal behaviour or lack of knowledge).
- A false sense of security, whereby security incidents are generally viewed as outsiders.
- Lack of information to report the incident, to minimise the damage (the person does not know who to contact).
- Feeling of shame for actions attributable to the security incident (e.g. negligence, deception, ignorance, inattention).

It is important to emphasise that the above aspects can be general and affect everyone (including us).

The target groups and forms

On the human side of cybersecurity, raising the level of security awareness requires a complex approach. The reasons for this include who the target groups for security awareness can be, either the wider society or an organisation, whose security awareness level can be understood as basically the sum of security awareness at the individual level. This immediately raises the issue of setting expectations at the organisational level, the need for commitment and support from senior management, and the need to raise awareness at the individual level. This approach focuses on methods and solutions that can be put at the service of security awareness. These can range from traditional awareness-raising solutions to training using professional and creative methods.

However, their content and orientation can vary considerably depending on the target groups. It stands to reason that the same depth and subject matter of "knowledge" is not required for a citizen facing cybersecurity threats in everyday life, for participants with professional level of involvement in dealing with them, or for participants with deeper IT knowledge.

For the latter, building on their existing expertise, it may be appropriate to strengthen the cybersecurity perspective. These often take the form of training courses, various specialised courses, but often in different areas of higher education.

This can have an impact on the design of appropriate programmes, where the different levels of basic knowledge, the expected level of motivation, generational

characteristics and the specific aspects of the workplace should be taken into account as a basic element. Knowing these as precisely as possible can increase the likely real success of programmes.

However, the effectiveness of awareness-raising training and programmes can be affected by a number of factors. The learning pyramid also shows, of course, that there are different rates of knowledge retention in different forms of training in each of the traditional (passive) teaching methods and teaming (active) teaching areas.

User and operator training is necessary when introducing different IT systems. However, in the case of post-deployment training, it is not only the necessary value-adding functions and information security requirements that need to be taught, but also the risk of incidents and their impact on confidentiality, integrity and availability.

To convey this responsibility and awareness, various information solutions and formats have been developed and are nowadays available in the form of security awareness programmes/training. The expectation is that these programmes will be able to communicate awareness in the most effective and sustainable way possible.

For those working in this field, the aim is to put in place and develop solutions that are as effective as possible and ensure that awareness is as sustainable as possible. Again, as a general truth, solutions that combine practical elements and delivery modes can be more effective, so shorter training sessions and, at higher levels, more complex cyber defence practice can be an evolving direction. Without going into the advantages and disadvantages of the different methods, it is clear that the design and delivery of practical methods is more time-consuming and often in limited circumstances (number of people, location).

Cybersecurity practices should be highlighted as an important part of improving the cyber resilience of organisations exposed to continuous and direct cyber threats. These secure and controlled environments can create opportunities to simulate real attack scenarios and allow participants to improve their technical skills by identifying previously unseen vulnerabilities or advanced attack methods. The experience gained from the exercises will help organisations to better understand their strengths and weaknesses. Cybersecurity exercises create the opportunity to identify weaknesses in the field and make an effective contribution to increasing cyber resilience.

On the awareness side, software development can be specifically mentioned. Software developers do not necessarily have the knowledge, skills and abilities to judge the extent to which they comply with secure coding guidelines (Gasiba et al. 2020). These flaws are largely brought to light during vulnerability assessments, software

security scans. However, the need and added value of coding in awareness warnings, in addition to functional and security testing, is already growing in software development.

Motivation

An important element of safety awareness programmes is the active, motivated attitude and participation of participants. This is often difficult to achieve, as participants often see participation in programmes as a compulsory element. Nevertheless, the tools for motivation can be wide-ranging (e.g. rewards), but most often they are not used.

Accordingly, the underlying aim is that participants leave such programmes not only "safer" but also with experiences that can be used at an individual level. This is where, among other things, the increasingly playful elements and forms of training (gamification), which are also visible in the literature, are valued. These can further increase the effectiveness of the programmes, either at individual level or in group form.

The advantages of the increasingly popular gamification approach are that its various forms can provide a specific framework (e.g. time limits, existence of "rules of the game", no real responsibility) for safety awareness programmes. Their advantages include:

- can increase the willingness to participate in programmes
- can contribute to a more permanent retention of information through their practical elements
- the results, including successes and failures, provide feedback to participants
- can enhance a more complex approach, interpreting the impact of action taken or not taken
- the opportunity to compete and form opinions without real stakes
- make participation an overall experience of success for the participants

The above may be a good indication that the development and application of appropriate methods of safety awareness is a complex task that requires continuous adaptation to the challenges of cyberspace.

Of course, it can also have a motivating effect if, for example, safety-conscious behaviour is counted as a plus in the annual performance appraisals of employees, and a minus if it is ignored. Of course, this is not intended to provide a cognitive understanding of the potential impact on the individual or organisation, but rather to measure the individual from the outside.

In our everyday activities in cyberspace, vulnerabilities that go back to human characteristics are constantly present. Mistakes, inattention, lack of motivation on the part of employees, but also deception and manipulation are mostly intentional, pose a serious risk in the field of cybersecurity. Being prepared for these, being aware of the threats in cyberspace and adopting the right behaviours can all contribute to reducing information security incidents, thereby increasing cybersecurity. Of course, for Digital Natives, Digital Immigrants (Prensky 2001), different areas of awareness training may lead to greater success. Those who are introduced to the use of IT tools early in life, who go through some "learning money", will experience their later conscious use differently.

Final thoughts

In the future, understanding the impact of threats from cyberspace, like physical space, will become a basic condition for "survival". Conscious behaviour, as a form of prevention, could be one of the main areas for enhancing security. However, this may not be given sufficient attention today, even though awareness and a security mindset need to be strengthened. There are, of course, many different levels and contexts for this, whether we are talking about taking account of generational specificities or finding appropriate forms of training and education for professionals, from the ordinary user. All in all, it is clear that cybersecurity, which is seen as a "technical area" for the ordinary person, cannot do without the importance of the human factor, which is at least as important as cybersecurity.

References

Gasiba, Espinha T. – Lechner, Ulrike – Pinto-Albuquerque, Maria – Fernandez, Mendez D. (2020): *Awareness of Secure Coding Guidelines in the Industry – A First Data Analysis.* 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, Guanzhou, China, 345–352. Online: https://doi.org/10.1109/TrustCom50675.2020.00055

Klein, Galit – Zwilling, Moti (2023): The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home. *Journal of Computer Information Systems,* 64(3), 408–422. Online: https://doi.org/10.1080/08874417.2023.2221200

Maalem-Lahcen, Ait R. – Caulkins, Bruce – Mohapatra, Ram – Manish, Kumar (2020): Review and Insight on the Behavioral Aspects of Cybersecurity. *Cybersecurity,* 3(10). Online: https://doi.org/10.1186/s42400-020-00050-w

Prensky, Marc (2001): Digital Natives, Digital Immigrants. Part 1. *On the Horizon,* 9(5), 1–6). Online: https://doi.org/10.1108/10748120110424816

Rantos, Konstatinos – Fysarakis, Konstantinos – Manifavas, Harry (2012): How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information Security Journal: A Global Perspective,* 21(6), 328–345. Online: https://doi.org/10.1080/19393555.2012.747234