Andrzej Pieczywok*

# Training employees on risks in the area of cybersecurity

**Abstract**

The title of the article points to an important area of human security as it relates to cyberspace as an environment for information exchange through networks and computer systems. In addition to the positive aspects, cyberspace also gives rise to various threats, such as cyber crises and cyber conflicts, cyber violence, cyber protests, or cyber demonstrations, including the threat of triggering a cyberwar. Risk is inherent in a given organization's cybersecurity. Therefore, one of the forms of counteracting this unfavorable phenomenon is periodic training among employees. In addition to an introduction, the article includes characteristics of cyberspace risk and suggestions for employee training in this area.

Key words: employee training, threats, cyberbullying, risk, cyberspace

* Assoc. Prof. Andrzej Pieczywok, PhD, Kazimierz Wielki University in Bydgoszcz, e-mail: a.pieczywok@wp.pl, ORCID: 0000-0002-4531-0630.

## Introduction

Modern society is described in terms of a risk society[1], which determines many phenomena (e.g. diseases, unemployment, armed conflicts, threats to security, including intellectual), which are a source of fears and anxieties. The scope and multiplicity of changes affecting human security have given rise to a hasty search for reform in all fields of human activity – including education. Didactics focused on active learning methods, experimental methods, project-based learning, and following various educational idols and gurus. Alternatives were continually sought.

The situation of modern people implies a level of risk that cannot be eliminated. Every action taken, choice made, trail blazed, stems from necessity and creates uncertainty. In „late" modernity risk is a permanent element of human activity. „To acknowledge the existence of risk as such, as the abstract systems of modernity force us to do to some extent, is to acknowledge and accept that our actions in no way follow a predetermined course and always remain open to adventitious events"[2].

Risk identification and assessment is an aspect of business decision-making that is often underestimated by entrepreneurs and managers. This is a difficult task due to the lack of complete and reliable information in a constantly changing market environment as well as within organizations.

Risk is inherent in safety. Just as there are many manifestations of risk, there are also many sides to the broad concept of security in business.

Security[3] is becoming an increasingly important aspect of daily online presence every year. Regardless of the industry, companies and institutions are processing ever-increasing amounts of data, and this automatically puts

**1** U. Beck, *Risk society: towards a new modernity*, London 1992; idem, *World Risk Society*, Cambridge 1994; idem, *Społeczeństwo ryzyka: w drodze do innej nowoczesności*, Warszawa 2004.

**2** T. Kaczmarek, *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2010, p. 41.

**3** See: M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018, p. 7; J. Gierszewski, A. Pieczywok, *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, vol. 9, p. 10–17; A. Pieczywok, *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018, p. 13; M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3; A. Pieczywok, *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021, p. 20–21.

them in the front row of potential targets for cybercriminals. That is why it is so important to educate employees not only about health and safety but also about cybersecurity. Cybersecurity training for employees of companies and institutions means knowing how to protect critical resources on company computers, awareness of the scale of threats associated with cyberspace, and the ability to implement good practices in information protection, among other things.

Cybercriminals are more and more often targeting companies and their employees, and hence security awareness training among employees is more important than ever. With intensive training provided both within and outside the organization, it is possible to develop a culture of security among employees, especially in terms of cyber threat awareness. Security training can be extremely valuable and save a company money in the long run, provided it is done right.

With training in the field of cybersecurity risk training, employees have a thorough understanding of threats associated with malware. In addition, they will learn how to use email safely, and how to protect themselves against spam. They will also learn about using electronic equipment safely, and how to create and store passwords securely. This will help them learn how to protect themselves from phishing and use social media safely.

Cybersecurity is seen as the prevention of damage, protection as well as the prospect of restoring the full ability to function properly of computers as well as electronic communication systems or specific communication services that takes place in cyberspace. On the other hand, it is also the protection of all the information that is included in the electronic communication space, and which ensures confidentiality while authenticating all authorized persons[4].

The most important goal and objective of cybersecurity is to protect cyberspace and all of its resources. Thus, it refers to the activities associated with the computer, the electronic communication system and the services that are performed with their help as well as with the use of electronic communications and information security. It includes protecting computer networks, responding to attacks, coordinating attack readiness, monitoring networks, and detecting or preventing attacks from occurring[5].

4 K. Midor, *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*, „Systemy Wspomagania w Inżynierii Produkcji" 2017, no. 6, p. 75–80.

5 Ibidem, p. 75–80.

It is also worth mentioning that the biggest threat to data security is the employees themselves – mainly current employees but also former employees or business partners, and suppliers, consultants, or vendors. Customer behavior can also be a source of danger. Most of these risks stem from a lack of awareness that a person is behaving irresponsibly. This is supported by the fact that companies that have chosen to implement cybersecurity awareness programs are most likely to report significantly lower financial losses incurred from irresponsible online activity by employees or others.

The purpose of this article is to highlight cyberspace risk issues and the training provided in an organization to employees in this area.

## Risk in cyberspace

Cyberspace is a complex environment resulting from the interaction of people, software, and services on the Internet through technical devices and their attached networks that do not exist in physical form[6].

Gradually, the term „cyberspace" began to be used by scholars to identify phenomena that are not products of human imagination, to name connections of a virtual nature[7].

Some authors define cyberspace as the interdependent network of information infrastructure that includes the Internet, telecommunications networks, computer systems, embedded processors, and controllers in strategic industrial environments[8], as well as copper cables, Internet routers, fiber optic cables, relay towers, and satellite transponders[9].

This understanding of cyberspace indicates that it is directly embedded in physical space through the entire ICT infrastructure. This type of definition is typically used to define so-called „state cyberspaces".

**6** *Open System Communications and Security, Telecommunication Security – Cyberspace security*, ITU-T X.1200–X.1299, Series X: Data Networks.

**7** R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [in:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, eds. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2014, p. 23.

**8** H. Katzan, *Cybersecurity Service Model*, „Journal of Service Science" 2012, vol. 5, no. 2, p. 72.

**9** M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, p. 82.

Pierre Lévy, French sociologist and author of the term „cyberculture", defines cyberspace as „a new space that enables communication, socializing, organizing, and transacting"[10]. The sociologist also points to the emergence of a new market for information and knowledge as a result of modern technological evolution. Cyberspace is the subject of study by social scientists, and references to the work of this academic discipline are found in some state cybersecurity strategies.

In the next view, the term „cyberspace" is used to refer to connections of a virtual nature created and operated by their physical manifestations – computers and telecommunications infrastructure. In this way of interpreting cyberspace, it is not uncommon to treat it as synonymous with the Internet.

Risk is a ubiquitous category in human activity and covers all its areas. It is not a homogeneous phenomenon, so it is difficult to give a single universal definition. Risk can be studied in objective and subjective aspects, keeping in mind, however, that it is a variable category, that is, more a process than a state of the external world. Thus, risk can be studied and defined depending on the specific aspect, framing, and context[11].

Risk pertains to core business areas, namely manufacturing, trading, and finance. In a market economy, goods are produced and services are provided and then sold, and both usually need to be financed. There are many divisions of risk in risk management theory. One is the division into strategic, operational, financial, personal, project, and insurance risks.

Risk stems from making decisions about the future. An individual or legal entity (company) undertaking diversified activities is uncertain of future results. Acting at risk due to an unknown future means making decisions in the absence of complete information. Risk and uncertainty occur side by side, occur together, and are sometimes equated.

The sources of risk are people who consciously make decisions, while dangers originate from outside and are difficult to influence. It turns out that more dangers than risks are now being created as a result of technological advances.

Man always lives in conditions of risk that are beyond their control or caused by them. In the past, the ability to control risk was limited. Man could

**10** P. Lévy, *Drugi potop*, http://portal.tezeusz.pl/cms/tz/index.php?id=287 [access: 20.02.2022].

**11** Confer: W. Tarczyński, M. Mojsiewicz, *Zarządzanie ryzykiem. Podstawowe zagadnienia*, Warszawa 2001.

not accurately identify causal relationships, and could not anticipate impending dangers or protect themselves from them. Hence, risk was associated with fatalism. Answers were sought outside of human capabilities, speaking of fate, the will of God, luck, bad luck, etc. Sometimes the explanation was individual initiative, cleverness, or enterprise.

In recent years, there has been increased interest in the study of risk in organizations in the context of cyber threats.

Cybercriminals have changed their tactics of operation. They are well aware that in the current situation, sudden changes to secure devices and servers can be very cumbersome. They use ransomware attacks. Files and documents are encrypted, making them difficult to access. They then require you to pay a fee to decrypt them. Unfortunately, many companies greenlight it, unable to afford the downtime.

The second type of attack used for financial gain is phishing. Taking advantage of the difficult situation in the world, they send crafted email, SMS, or messages using instant messengers such as Messenger or Whatsapp trying to impersonate a trusted source, which may be a government organization, financial institution or the World Health Organization (WHO), forcing the recipient to click on a link or attachment containing or leading to an infected website.

All kinds of security vulnerabilities in programs and applications are also very common. Due to companies' security policies that are not adapted to continuous remote operation, many of them do not have the latest updates, so they have become a very popular target for attacks.

The category of risk, to which A. Giddens refers, is not limited only to the new threats that currently appear before man (cyber attack, cyber warfare, etc.), but he treats it as a certain attitude towards reality, which he explains as follows: „to live in a risk society is to live with an analytical attitude toward the possible courses of action, positive and negative, that, as individuals and globally, we face in the course of our social existence". The risk is all the greater because the term „control" has been devalued, for: „change exceeds all human expectations and is out of human control"[12]. Risk is therefore inherent in the life of modern man, accompanying them in everyday life. We should even talk about being aware of the risks that accompany all their initiatives and actions,

**12** A. Giddens, *Nowoczesność i tożsamość. „Ja" i społeczeństwo w epoce późnej nowoczesności*, Warszawa 2001, p. 40–41.

even when everything goes according to plan. The individual today must live with the knowledge that something can go wrong, that something could not be foreseen, and that something can always surprise.

In a risk society, an employee must possess specific skills and abilities to function efficiently in that society. „What becomes important here is the ability to anticipate dangers, to tolerate them, to deal with them in a biographical and political sense"[13]. An employee in an organization today must be able to calculate the risks, opportunities and threats they face in cyberspace.

## Training employees on risks in cyberspace

Extracurricular activities aimed at acquiring, supplementing, or simply improving the skills and professional qualifications of employees are usually called training. It pertains to both doing the job and looking for it.

According to J. Misztal, the concept of training should be understood as a set of activities that are systematically aimed at deepening and broadening the capabilities of the employee[14]. In her book, J. Moczydłowska defines training as: „a short-term educational activity designed to develop in an individual the knowledge, skills, and attitudes necessary to meet current and future job-specific requirements"[15]. It is worth pointing out the definition of training by M. Kostera, which defines training as „the process of complementing knowledge by an employee, necessary for them to properly perform the tasks at their position, creates for them a possibility not only to acquire specific information or skills but also allows promotion in the organization. Education and development foster the broadening of an employee's horizons, the development of personality traits such as innovation and entrepreneurship, and the satisfaction of an employee's needs for self-actualization"[16].

How employee training is defined has significant implications on the functions of training in an organization. These functions are as follows: 1) adaptive function – involves adapting the employee's knowledge and skills to the requirements of the job. Training courses performing these functions

**13** Ibidem, p. 98.
**14** A. Pocztowski, *Zarządzanie zasobami ludzkimi. Zarys problematyki i metod*, Kraków 1998, p. 225.
**15** J. Moczydłowska, *Zarządzanie zasobami ludzkimi w organizacji*, Warszawa 2010, p. 81.
**16** M. Kostera, *Zarządzanie personelem*, Warszawa 1999, p. 47.

are intended for all new hires and those who need to adapt to changes in the content of work occurring under the influence of technical and organizational progress; 2) modernization function – related to the need of renewing qualifications that over time become obsolete due to advances in science and technology, or need to be refreshed due to routine. Training performing this function improves the employee's well-being, allows them to feel competent at their position, but unfortunately does not ensure further promotion; 3) innovative function – it consists in creating conditions for creating progress, favors the introduction of new solutions. Training performing this function involves employees who can affect the way the organization operates; make decisions or will be promoted in the future; 4) social function – is to strengthen ties between people, involves learning to cooperate.

This is especially true for developing interpersonal skills that will be used to improve internal interactions among employees as well as with customers. Training is also meant to integrate employees toward the common goals of the organization[17].

Training objectives can be considered depending on whether the subject is the company or the employee. From the point of view of the needs of the enterprise, training an employee as an element of the organization is, as A. Sajkiewicz writes, the „creation of such systems of labor potential development that contribute to increased competitiveness, and thus to the survival and development of the organization. Although the direct purpose of employee training is to increase competitiveness, training can also create a learning organization model"[18].

In the available literature, we can find several divisions of training types. One of them is the division between mandatory (obligatory) and optional (facultative) training.

Mandatory (obligatory) training – this is training resulting primarily from the provisions of the labor law, which apply to all employees, both those who are starting work as well as those who are already employed, and these are e.g. OSH training, fire safety training, workplace training, or from separate provisions of the law, which apply to e.g. auditors, teachers, accountants. These are usually training courses specialized in a particular field, aimed at

**17** *Zarządzanie zasobami ludzkimi w warunkach nowej gospodarki*, eds. Z. Wiśniewski, A. Pocztowski, Kraków 2004, p.177.

**18** S. Sajkiewicz, *Zasoby ludzkie w firmie*, Warszawa 2003, p. 252.

improving the skills of a particular group of employees and often conditioning further work in a given position or the company.

Optional (facultative) training – specialized training that allows supplementing the necessary knowledge and skills, it is not required by the employer and does not arise from the needs of the job but it improves the qualifications of the employee and may affect their further personal development and career. The employee shall register their participation in such training and pay the cost of attendance themselves. These training sessions are short refresher meetings held after business hours.

As part of ongoing employee training regarding risk in cyberspace, basic industry standards to secure sensitive data should include: 1) limited trust – the „never trust, always verify" rule; 2) identity management and control of access to corporate resources; 3) VPN – a solution used in corporate networks to provide a secure, encrypted connection to corporate resources; 4) software updates.

The most important element, of course, is having a skilled IT staff. Even the best security measures can be ineffective when the person monitoring them is not experienced. The assistance of specialists who perform phishing tests, security audits, provide information and training measures for employees allows to identify vulnerabilities of the infrastructure already in place and reduce the risk of data loss

The training provided should mainly focus on examples of hacking attack patterns, and the dangers of using the Internet using simple and understandable language. In addition, there should be a definition of what social engineering is and why it is so dangerous. Employee training on cyber risks should aim to raise employee awareness with examples presented. The trainer should give clear theoretical knowledge and examples of hazards, which has a great effect on stimulating the imagination of the employee, making them more cautious about hazards. At the end of the training, the employee should have the skills to deal with online threats, develop an appropriate reaction to them, and know how to recognize them. The trainee should gain knowledge of „good practices" and maintaining „cyber hygiene" in handling electronic devices. The training should also include information on how a hacker can use stolen personal information – this stimulates the imagination of the recipient by identifying with the victim.

To consciously address the topic of security with respect to cyber risk requires a sound risk analysis that takes into account the business context of the organization. Periodic audits and security testing are necessary. A company needs to know what impact certain types of threats will have on

the smoothness of its business processes. Building safety policies and training and sensitizing employees are necessary, but education alone is not enough to significantly reduce risk levels. Security policies should be the beginning and the basis of technology selection. Hard technology solutions are needed because the complexity of tasks faced by employees is too great to remember everything. Even large and trained security teams cannot properly respond to threats without the right tool support.

The bottom line is that businesses today are exposed to a variety of cybersecurity threats, and the rise of remote working over the past year has only exacerbated them. Clearly, the most effective way to mitigate corporate cybersecurity threats is to periodically implement cybersecurity training. The training must be engaging for employees or employees will continue to be vulnerable to cyberattacks.

**Bibliography**

Aleksandrowicz R., Liedel K., *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [in:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, eds. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2014.

Beck U., *Risk society: towards a new modernity*, London 1992.

Beck U., *Społeczeństwo ryzyka: w drodze do innej nowoczesności*, Warszawa 2004.

Beck U., *World Risk Society*, Cambridge 1994.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Giddens A., *Nowoczesność i tożsamość. „Ja" i społeczeństwo w epoce późnej nowoczesności*, Warszawa 2001.

Gierszewski J., Pieczywok A., Społeczny wymiar bezpieczeństwa człowieka, Warszawa 2018.

Kaczmarek, T. *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2010.

Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, vol. 9.

Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3.

Katzan H., *Cybersecurity Service Model*, „Journal of Service Science" 2012, vol. 5, no. 2.

Kostera M., *Zarządzanie personelem*, Warszawa 1999.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Lévy P., Drugi potop, http://portal.tezeusz.pl/cms/tz/index.php?id=287 [access: 20.02.2022].

Midor K., *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*, „Systemy Wspomagania w Inżynierii Produkcji" 2017, no. 6.

Moczydłowska J., *Zarządzanie zasobami ludzkimi w organizacji*, Warszawa 2010.

Pieczywok A., *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018.

Pieczywok A., *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021.

Pocztowski A., *Zarządzanie zasobami ludzkimi. Zarys problematyki i metod*, Kraków 1998.

Sajkiewicz S., *Zasoby ludzkie w firmie*, Warszawa 2003.

Tarczyński W., Mojsiewicz M., *Zarządzanie ryzykiem. Podstawowe zagadnienia*, Warszawa 2001.

*Zarządzanie zasobami ludzkimi w warunkach nowej gospodarki*, eds. Z. Wiśniewski, A. Pocztowski, Kraków 2004.

# Szkolenie pracowników na temat ryzyka w obszarze cyberbezpieczeństwa

**Streszczenie**

Treść artykułu wskazuje na istotny obszar bezpieczeństwa człowieka, dotyczy bowiem cyberprzestrzeni jako środowiska wymiany informacji za pomocą sieci i systemów komputerowych. Cyberprzestrzeń oprócz pozytywnych zjawisk powoduje też powstawanie różnych zagrożeń takich, jak: cyberkryzysy i cyberkonflikty, cyberprzemoc, cyberprotesty czy cyberdemonstracje, w tym także groźba wywołania cyberwojny. Ryzyko nieodłącznie związane jest z cyberbezpieczeństwem w danej organizacji. Dlatego też jedną z form przeciwdziałania temu niekorzystnemu zjawisku są cyklicznie realizowane szkolenia pracowników. Artykuł oprócz wprowadzenia zawiera charakterystykę ryzyka w cyberprzestrzeni oraz propozycje szkoleń w tym zakresie pracowników.

**Słowa kluczowe:** szkolenie pracowników, zagrożenia, cyberprzemoc, ryzyko, cyberprzestrzeń