The importance and challenges of information security in the digital age: analysis of the current situation and prospects for development

Aleksander Sapiński[1]

[1] Bielsko-Biala School of Finance and Law
Poland

***Abstract*— In this age of increasing digitalisation, information security is becoming one of the most important issues for every state and organisation. This article provides an analysis of the current situation of information security and the challenges it faces. The article focuses on various aspects of information security, such as cyber security, privacy protection, data protection and network security. It also analyses the ways in which countries and organisations are taking steps to ensure information security and the challenges that accompany these efforts. Finally, the article provides an outlook on the development of information security in the digital age and points to the most important directions to be taken to ensure information security in the future.**

Keywords— security studies, information security, digital age, information security management.

I. INTRODUCTION

Information is becoming one of the most valuable assets of any organisation or state and is becoming increasingly guarded and valued. At the same time, this information is exposed to many threats, such as cyber-attacks and breaches of data privacy. Therefore, information security has become one of the most important issues for anyone using ICT. It is worth noting that these threats do not only affect large companies and state institutions, but also ordinary users who process and store their data online.

This article aims to provide an overview of the current situation of information security and the challenges it faces. Various aspects of information security will be presented, such as cyber security, privacy protection and network security. The most important information security challenges affecting both states and private organisations will also be discussed. Furthermore, the article will focus on the prospects for the development of information security in the digital age.

It is important to emphasise that information security is a global issue and affects every country in the world. According to a report published by Accenture and Ponemon Institute, the cost of information security breaches in 2020 averaged $3.86 million per organisation (Accenture 2020 p.1-16). In addition, there were more than 300 billion cyber-attacks worldwide in 2020. These figures show how important it is to take care of information security and how real the threats posed by cyber-attacks are.

The number of cyber-attacks has increased over the past few years, which in turn has raised people's awareness of the need for information security. In 2020, companies around the world were forced to adapt to the COVID-19 pandemic and conduct their operations online, which further increased the risk of cyber-attacks. Many organisations have been forced to rapidly digitise their business processes, which has increased the threat of hacker attacks.

In addition, with the development of technology, new threats are emerging, such as attacks on artificial intelligence, mobile applications, IoT systems and many others. In order to deal with these threats, companies and institutions must take steps to increase their levels of information security.

II. DEVELOPING A DEFINITION OF INFORMATION SECURITY IN THE CYBER WORLD

Information security is a comprehensive system of measures designed to protect information from unauthorised access, disclosure, damage, destruction, modification or loss. In today's digital age, where information is transmitted via the Internet, information security has become a key element for both organisations and individuals (ISO 2013).

The authors of the definitions of information security and

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 27, No 1 (2023), pages 4
https://doi.org/10.19192/wsfip.sj1.2023.8
Received: October 2022 Accepted: April 2023
Published: March 2023

cyber security are not clear-cut, as both terms have their roots in a number of scientific fields, including computer science, management and national security. One of the first authors to define the term cyber security was Dorothy Denning (Denning, 1999), an American computer security specialist.

The definition of information security refers to the protection of information from unauthorised access, disclosure, damage, destruction, modification or loss. Cyber security, on the other hand, is more focused on the protection of digital information and related systems from threats arising from computer networks (ENISA, 2021).

With the development of information technology, these terms have come to be used interchangeably. However, there are some subtle differences between the two. Cyber security refers to efforts to protect networks and related systems from digital threats such as hackers, viruses, DDoS attacks, etc. Information security, on the other hand, refers to the protection of all types of information, not just that stored in IT systems.

The dangers of information in security are serious and can lead to severe consequences such as invasion of privacy, identity theft, loss of commercial and confidential information and even reputational damage. As research shows, the costs associated with cyber-attacks are increasing, and their scale and complexity continue to grow.

According to IBM Security's 2020 Cost of a Data Breach Report, the cost of an average data breach was $3.86 million in 2020, an increase of 1.5 per cent over the previous year (IBM Security, 2020). Also, Microsoft's 2020 Digital Defense Report states that cybercrime is one of the biggest threats to businesses and individuals, and that the cost of losses associated with cyber-attacks was more than $1.5 trillion in 2020(Microsoft, Digital Defense Report, 2020).

In Europe, the European Network and Information Security Agency (ENISA) publishes an annual report on network and information threats. In its Threat Landscape Report 2021, ENISA states that there was an increase in malware, phishing and ransomware attacks in 2020, highlighting the need for action to improve information security.

III. The various aspects of information security

Information security is crucial to the functioning of modern societies. Protecting information from unauthorised access, theft or destruction is one of the most important tasks of businesses, government organisations and other institutions. In this article, we will discuss various aspects of information security.

IV. Technical aspects

Information security involves many technical aspects. Information systems, networks and databases must be adequately protected against cyber-attacks. Today's attacks can range from viruses and worms to phishing, ransomware and DDoS (Distributed Denial of Service) attacks. Attackers use a variety of means, such as password phishing, zero-day attacks and even social engineering, to gain access to protected information (Bonner, 2020).

Securing IT systems requires the use of various tools and technologies, such as firewalls, anti-virus, anti-spam and anti-phishing software. It is also important to regularly update software and follow security best practices such as complex passwords and regular staff training.

V. Legal aspects

Information security is also regulated by law. Many countries have data protection laws and require companies and government institutions to comply with certain information security standards. In Poland, such regulations include the Personal Data Protection Act and the GDPR (Regulation on the Protection of Personal Data). In the US, similar legislation is regulated by the Computer Fraud and Abuse Act (CFAA), among others (Jankowski, 2018.).

VI. Organisational aspects

Information security also requires proper work organisation in companies and institutions. A properly organised IT infrastructure and proper security procedures help to ensure information protection (Stachowiak, 2019). Data access procedures should be in place, backups secured, and data minimisation policies implemented to reduce the risk of information leakage.

IV. Current situation of information security.

Information security is currently one of the most important challenges for many institutions, businesses and organisations around the world. Attacks on IT systems can lead to the loss of sensitive information such as customer data, employees, passwords and other sensitive information. Recent years have seen many instances of attacks on information systems, which have sparked a wave of discussion about the need for increased information protection and security measures.

A. Examples of attacks on information systems

One of the largest attacks on information systems was on Equifax, which is one of the three major credit reporting bureaus in the United States. In 2017, hackers accessed the personal data of more than 147 million customers, including national insurance numbers, dates of birth, addresses and other information. The attack was one of the largest in history and caused serious financial and reputational damage to Equifax.

Another example was the 2013 hacking attack on US company Target, which caused many companies to rethink their approach to security. As a result of the attack, hackers gained access to the data of more than 110 million customers, including credit card numbers and personal information. The attack caused losses of more than $162 million.

VII. Action taken by countries and organisations

Governmental and non-governmental organisations around the world are taking a number of measures to enhance information security and protect against cyber-attacks. In 2018, the European Network and Information Security Agency (ENISA) issued a report identifying several key information

security risks, such as attacks on critical infrastructure, the use of blockchain technology for criminal purposes and attacks on cloud systems. In response to the growing threats, countries around the world are taking many measures to increase the protection of their information systems. In Poland, the Internal Security Agency (ABW) is working with various institutions to raise awareness of cyber threats threats and preventive measures. The agency conducts training for businesses and government institutions and organises information campaigns on information security. In 2020, the National Security Agency launched a special 'Safe Company' website, which provides practical advice and information on information security for businesses. Other countries are also taking similar steps. In the United States, the National Institute of Standards and Technology (NIST) has developed the Cybersecurity Framework, which is a set of recommendations and best practices for information security. In Europe, the European Network and Information Security Agency (ENISA) is developing recommendations on information security and organising training and awareness campaigns. International organisations are also taking steps to enhance information security. An example is NATO, which has developed the concept of cyber defence and provides training for its members on information security.

It is worth noting that protecting information systems and data is not only the responsibility of states and organisations, but also of individual users. Examples of good practice include using complex passwords, updating software regularly and being careful when opening suspicious messages or clicking on links.

More and more activities shifting to the digital world, information security risks pose a serious challenge to societies around the world. In response to these challenges, countries, organisations and individual users are taking various measures to increase the protection of data and information systems. It is important to remember that taking care of information security is everyone's responsibility.

V. Challenge for information security

One of the biggest challenges to information security is the lack of a uniform information security policy. Each country, organisation or company has its own approach to information security management. These differences can be due to many factors, such as cultural, legislative, organisational or technological differences. An insufficiently harmonised approach to information security management leads to an information security vulnerability that can be exploited by an attacker. Therefore, it is important for countries, organisations or companies to operate on the basis of harmonised information security standards (Kuhn 2010).

Threats related to the development of technology pose another challenge to information security. As technology advances, attackers have more and more opportunities to launch cyber-attacks. An example of such a threat is the developing technology of artificial intelligence, which allows the creation of tools to carry out attacks with even greater precision and efficiency (Pope 2005). Additionally, the increasing number of network-connected devices, such as IoT devices, increases the number of potential attack vectors. This requires countries, organisations and companies to continually work to secure their systems against new types of threats (Chakrabarti, 2010).

One way to deal with information security challenges is to develop threat monitoring and response systems. Such systems make it possible to detect attacks quickly and take appropriate action to minimise the impact of the attack. In addition, developing employees' information security competence and awareness is key to ensuring effective protection of systems. States, organisations and companies should invest in training and information security education for employees so that they can effectively protect their systems from cyber threats (Scarfone and Mell, 2007).

VI. Prospects for developing information security

The increasing number of cyber-attacks, which are becoming more and more advanced, as well as new threats related to the development of technology, require the continuous development of measures to ensure information security. It is worth considering what are the prospects for the development of information security, what are the most important directions of development and what is the role of the state and organisations in ensuring information security.

The state and organisations play a key role in ensuring information security. In Poland, the Internal Security Agency (ABW) is responsible for coordinating activities related to information security, as well as for carrying out activities related to the protection of classified information (Swoboda, 2014, p.303). In addition, various government institutions and agencies monitor the information security situation and take measures to prevent threats.

Organisations also need to effectively secure their IT systems against cyber-attacks, which can lead to data theft, malware or damage to systems. To do so, they need to use advanced information security technologies and practices and conduct regular security audits.

Developments in information technology are creating new opportunities, but also new threats to information security. With the development of the Internet of Things (IoT), artificial intelligence (AI) and blockchain, the number of potential attacks on information systems is increasing. One of the biggest challenges will be to ensure the security of systems managing large amounts of data, such as medical, financial or critical infrastructure-related data. However, developments in information technology are also creating new opportunities for ensuring information security. For example, artificial intelligence can help to detect and prevent and prevention of attacks, and blockchain in securing systems against unauthorised access. In addition, the development of the Internet of Things (IoT) and other technologies related to the industry 4.0 concept may allow better monitoring and management of IT systems in real time, which in turn will have a positive impact on information security (Pope, 2004, p.233-240).

Cybersecurity education and training is also an important direction for the development of information security. Knowledge of threats and how to avoid them should be widespread, both among individual users and among businesses and public institutions. Therefore, states and organisations should invest in training programmes and education campaigns to raise awareness of cyber threats and how to counter them (Sobers 2022).

States and organisations also have a key role to play in creating uniform information security standards that will apply internationally. Many countries are developing their own information security regulations, which leads to inconsistencies and hinders international cooperation in the event of attacks on information systems (Varnois 2022). One example of such cooperation is the European Network and Information Systems Directive (NIS), which aims to ensure a high level of security for information systems in European Union member states (Symantec 2020).

In summary, the development of information technology creates both new threats and opportunities for information security. States and organisations have a key role in ensuring security and should invest in education and training, the creation of uniform standards and the implementation of innovative technological solutions (Wright et all, 2023).

VII. Conclusion

Information security is a key aspect in the digital age. Inadequate data management and proteronie can lead to serious consequences, including information leakage, identity theft or threats to privacy. As a result, countries and organisations around the world are taking many steps to ensure the protection of their information systems. One of the biggest challenges to information security is the lack of a uniform information security policy. Differences in approaches to information security management between countries, as well as within organisations, pose a significant threat. In response to this problem, more and more countries and organisations are adopting information security standards and guidelines.

However, developments in information technology are also creating new opportunities for ensuring information security, such as the use of artificial intelligence in detecting and preventing cyber-attacks or the development of blockchain solutions to secure transactions and transmitted data. Therefore, countries and organisations should continue their efforts to protect their information systems and work towards a unified information security policy that takes into account changing technologies and threats. (Szczypiorski 2019). At the same time, developing new technologies and innovative solutions can improve information security in the digital age.

VIII. References

Accenture, Ponemon Institute (2021) *Cost of Cybercrime Study: Global*, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Cybersecurity Ventures (2020) *Cybercrime Report 2020*, https://cybersecurityventures.com/cybercrime-report-2020/

IBM Security (2020) *Cost of a Data Breach Report*, https://www.ibm.com/security/data-breach

Microsoft (2020) *Digital Defense Report*, https://www.microsoft.com/security/blog/2020/10/12/digital-defense-report/

European Union Agency for Cybersecurity (2021), *Threat Landscape Report 2021*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2021

IBM Security (2020) *Cost of a Data Breach Report*, https://www.ibm.com/security/data-breach

S.E. Bonner (2020) *Cybersecurity Essentials*. Packt Publishing Ltd.

D.E. Denning (1999) *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services*, US House of Representatives.

ISO/IEC 27001:2013 *Information technology -- Security techniques -- Information security management systems Requirements*, International Organization for Standardization (ISO), 2013.

D. Florêncio & C. Herley (2007) *A Large-Scale Study of Web Password Habits*, In Proceedings of the 16th International Conference on World Wide Web, Banff, AB, Canada.

M. Jankowski (2018) *Bezpieczeństwo informacyjne w przedsiębiorstwie*, Wydawnictwo Naukowe PWN.

A. Stachowiak (2019) *Bezpieczeństwo informacyjne w organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej.

"NATO's Cyber Defence, https://www.nato.int/cps/en/natohq/topics_78170.htm.

J. Kuhn (2005), *Different Approaches to Information Security Management*, in Proceedings of the 38th Hawaii International Conference on System Sciences

K. Scarfone and P. Mell (2007) *Guide to Intrusion Detection and Prevention Systems (IDPS),* National Institute of Standards and Technology, Special Publication 800-94.

P. Swoboda (2014) *Agencja Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa państwa*, Bezpieczeństwo RP wczoraj i dziś, (ed.) M. Śliwa, A. Żebrowski, R. Kłaczyński, Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego.

J. Chakrabarti (2010) *Security in the Cloud: Challenges and Opportunities*, in Proceedings of the 2010 International Conference on Advances in Computing, Communications and Informatics

A. Jøsang and S. Pope (2004) *Formal Requirements for Virtual Organizations*, in Proceedings of the 5th IFIP WG 8.5 Working Conference on Virtual Enterprises.

K. Szczypiorski (2019), *Cyberbezpieczeństwo. Zagrożenia i wyzwania*, Politechnika Warszawska, Warszawa.

D. Wright, N. Tomić, S. Portesi, L. Marinos (2023), *ENISA cybersecurity market analysis framework v. 2.0* available at: https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0