Information and Computer Literacy

Nena Orel Šanko
University of Maribor, Faculty of Logistics, Celje, Slovenia
nena.orel@um.si

Today, information and computer security are extremely important for several reasons. Digitalisation has enabled a massive flow of data and information through computer networks, where information is often sensitive in nature, including financial data, personal identities, and business secrets. It is imperative to protect information from unauthorised access and misuse. In today's digital world, a lot of infrastructure is connected to computer networks, such as schools, hospitals, and transportation systems. Attacks on these systems can lead to significant financial or material damage and jeopardise people's lives. Hence, it is crucial to ensure systems' security and resiliency against cyber-attacks, which have become increasingly common, sophisticated, and exploit vulnerabilities to steal data, spy, and cause harm. Thus, constant upgrading of security measures and raising awareness among people are essential. Therefore, information and computer security are of paramount importance for safeguarding privacy, economic stability, and national security in the modern digital world.

DOI
https://doi.org/10.18690/um.fl.2.2026.3

ISBN
978-961-299-074-9

Keywords:
information security,
computer security,
data,
information

University of Maribor Press

1 Introduction

Information and computer security have become fundamental issues in today's digital age, where data and information have become valuable resources that drive both private and business environments. With the rapid development of technology and constant connectivity via the Internet, data protection has become crucial, as new threats have emerged that threaten both individuals and organizations. Security breaches such as identity theft, hacker attacks and loss of sensitive information may result in serious consequences that can cause irreparable damage on both a personal and business level. Therefore, ensuring information and data protection is a key task today, which ultimately protects our privacy, financial stability and business competitiveness.

At the beginning, it should be made clear that the existence and operations of every organization depend on information technology (hereinafter: IT) resources, without which logistics processes and supply chain systems cannot (smoothly) operate (Jereb, 2017). These include (Kajba et al., 2023): information, applications (or software), infrastructure, intangible assets, and people. IT resources are available for implementation in various IT processes (Jereb, 2017), and we can understand them as investments in these processes, where the appropriate level of protection is also important (Jereb et al., 2016). We can also argue that these four IT resources are the foundation of every technology, constituting four interdependent, co-determining and equally important components (Kabanda, 2019).

For each of the IT resources, it is also necessary to ensure the IT requirements that were already mentioned in the chapter "Digitalization – Planning". According to the Control Objectives for Information and related Technology, there are seven business requirements or information criteria for IT resources (IT Governance Institute, 2007):

- effectiveness – refers to information relevant to the business process that is part of that business process and its timely provision, correctness, consistency and usability,
- efficiency – refers to providing information with optimal use of resources,
- confidentiality – refers to protecting sensitive information from disclosure,

- integrity – refers to the accuracy and completeness of information and its validity in accordance with business value and expectations,
- availability – refers to information that must be available when needed in business processes and the protection of necessary resources and related capabilities,
- compliance – addresses compliance with laws, regulations and contractual agreements (externally defined business criteria, internal policies) that apply to the business process in question,
- reliability – refers to providing management with appropriate information to manage the organization and carry out its responsibilities for confidentiality and governance.

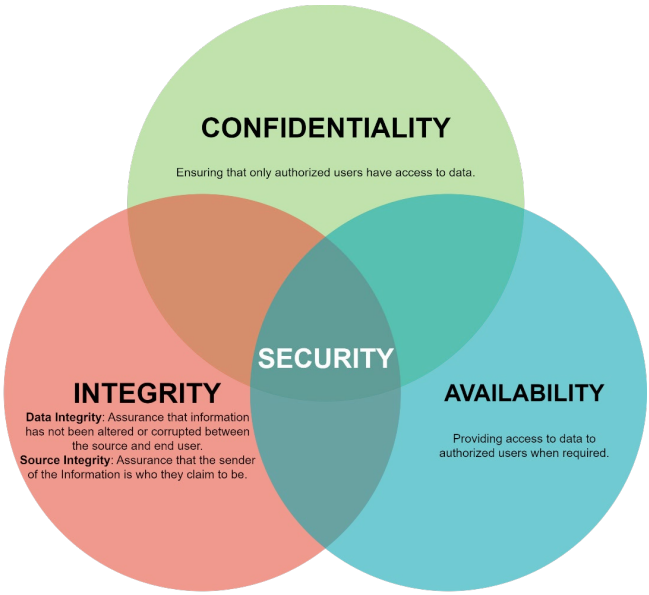

Figure 3.1: The CIA Triad
Source: own.

Informatics, from a security perspective, primarily requires that information is available, complete and confidential to the extent necessary to implement and support business processes. In the case of logistics, this means ensuring the availability, completeness and confidentiality of information so that the right products or services can be provided in the right quantity and quality, delivered to the right place and at the right time (Kajba & Jereb, 2021). These three requirements

(availability, completeness and confidentiality) also make up the CIA Triad (Figure 1.1), where (Kemmerer, 2003):

- confidentiality ensures that sensitive information is not disclosed to unauthorized recipients,
- integrity ensures that data and programs are modified or destroyed only in a specific and authorized manner,
- availability ensures that IT resources will be available whenever an authorized user needs them.

2 Types of Security and Threats Related to IT Operations

The chapter "Digitalization – Planning" outlined the general importance of information and cybersecurity, describing the key elements of cybersecurity and proactive and comprehensive approaches. The following is a detailed description of the various types of security and IT threats.

2.1 Types of security related to IT operations

It is necessary to introduce the types of security related to IT operations: information security, IT security, cybersecurity, computer security and network security.

Information Security (InfoSec) encompasses the tools and procedures that organizations use to protect information and prevent unauthorized access to business or personal information, including policy settings that prevent unauthorized people from accessing business or personal data. InfoSec is a growing and evolving field that covers many aspects from network security testing, auditing, and infrastructure. It protects sensitive data from unauthorized activities, including viewing, modifying, recording and any disruption or destruction. The main goal is to ensure the security and privacy of critical organizational data, such as: customer account details, financial data or intellectual property. Organizations must allocate resources to ensure information and data security and be prepared to detect, respond to, and proactively prevent attacks such as: phishing, malware, viruses, malicious insiders, and ransomware ('Information Security: The Ultimate Guide', n.d.).

Information Technology Security (IT security) describes precautions taken to protect computers and networks from unauthorized access. Procedures and processes are designed to prevent data theft or disruption of information systems. High-quality IT security focuses on protecting data integrity, maintaining the confidentiality of information stored on a network, ensuring that data and information are accessible to authorized personnel, verifying the authenticity of users attempting to access computer networks, and enabling secure messaging across networks for users (The Upwork Team, 2021).

While both IT security and cyber security focus on protecting customer data, they take slightly different approaches. IT security refers to a broader understanding of security, exploring the steps to protect business data, including physical data and information in internal systems. Cyber security focuses more on the threats an organization may encounter over the Internet when information and data are transmitted digitally or otherwise used online (The Upwork Team, 2021). Cyber security encompasses a set of tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, best practices, assurances, and technologies that can be used to protect the cyber environment and the assets of the organization and its users (Von Solms & Van Niekerk, 2013).

Computer security generally focuses on protecting computer systems from unauthorized access and use. Computer security professionals work to establish best practices for computer security, which include managing computer and network security and creating a culture focused on security within the organization. There are several types of computer security that affect different elements of an organization's physical and digital infrastructure. As a result, there are a wide variety types of security that professionals need to focus on, including (The Upwork Team, 2021; 'What Is Computer Security?', 2022):

- application security – describes the steps developers take when building an application to ensure user security and reduce vulnerabilities in the application (this type of security involves analyzing the application code to find potential weaknesses),
- information security,

- network security – protects an organization's digital infrastructure and prevents security incidents on computer networks so that users can work without interruption,
- internet security – protects browsers and information in applications that use the Internet. Firewalls and similar types of protection that only allow authorized users to access protected areas are considered internet security services,
- cloud security – ensures that users connecting through cloud applications remain protected and uses systems such as cloud-based unified threat management (UTM) to maintain secure cloud connections,
- operational security – describes the practices and analysis used in routine activities to find potential vulnerabilities that hackers can exploit. The goal is to see regular actions from the perspective of a bad actor and identify where they can take advantage,
- endpoint Security – with the number of devices used in an organization (mobile phones, tablets, laptops, and computers), endpoint security focuses on protecting these system endpoints and includes protecting devices from malware infection.

Each of these types of computer security includes multiple components, which makes them a specialized field in their own right. ('What Is Computer Security?', 2022). The aforementioned CIA triangle has been the industry standard for computer security since the development of the mainframe[1] (Whitman & Mattord, 2011).

Understanding the difference between IT security and network security lies in understanding the different uses of data. IT security focuses on all data managed by an organization, while network security focuses on network systems and protecting them from intrusions and data attacks. Security service providers often protect the infrastructure that enables organizations to collaborate electronically (The Upwork Team, 2021).

[1] Mainframe - at their core, "mainframes" are high-performance computers with large amounts of memory and data processors that process billions of simple calculations and transactions in real time (IBM, n.d.).

2.2 Types of IT threats

Before we continue with types of hacks, it is necessary to mention the types of IT security threats (The Upwork Team, 2021):

- cybercrime – involves the targeting or use of computers or computer systems to commit crimes (identity theft or extortion) for some type of financial reward,
- cyberattacks – large-scale digital attacks that can disable an entire computer system or multiple computer systems (attacks may use malware or ransomware) to achieve the goal of obtaining information about millions of users or carrying out a denial of service (DoS) attack,
- cyberterrorism – uses the tools and methods of cybercrime and attacks to attempt to target the critical infrastructure of countries or otherwise harm countries and cause fear through unauthorized access to communications infrastructure.

3 Malicious software

A common term for malicious software is also malicious code or "malware". Every year, businesses are flooded with malware attacks, caused by the ever-increasing communication capabilities of computers and phones. A characteristic of all forms of malware is that their existence is unwanted, unknown or hostile to the attacked user who receives these programs. Twenty years ago, malicious code spread exclusively via floppy disks that users transferred from computer to computer. With the increase in communication capabilities, the prevalence of malicious code has also increased. Today, pests like to spread via files, e-mail, instant messaging systems and websites (Šepec, 2018).

Malware exploits security vulnerabilities in operating systems and applications to spread infections. The successful penetration of malicious code is a result of the inadequacy of traditional defense tools, which operate primarily reactively. Antivirus and antispyware programs are most successful in combating attacks. When a new type of malware appears on the Internet, it can spread unhindered until antivirus vendors analyze the attack and create a suitable “vaccine.” Properly configured firewalls could play a vital role in this fight; however, most users do not even know what a firewall is.

3.1 Types of malware

Malware appears as an auxiliary or main means of execution in many cybercrime crimes and is defined as harmful programs especially adapted for attacks (damage) on information systems, networks or data (Šepec, 2018). In today's information age, in which the possibility of profiling individuals is relatively common and interference with the information privacy of individuals has reached the highest level in history, spyware is anything but an innocent collection of codes. Malicious codes, which dominate criminal acts, and through which a variety of methods can be implemented, cause various disruptions, damage and serious obstruction of information systems and e-data. A characteristic of all forms of malware programs is that their existence is unwanted, unknown or hostile to the attacked user who receives these programs (Šepec, 2018).

When cybercriminals plan to attack computer networks and systems, they have a variety of tools at their disposal. There are several types of malicious attacks that organizations should be aware of when developing their cybersecurity and IT security strategies. Some of the types of malware are presented below: viruses, worms, Trojan horses, spyware, adware, ransomware, and (distributed) denial of service.

3.1.1 Viruses

The word VIRUS stands for »Vital Information Resource under Siege« (Maity & Dey, 2021). While all types of malwares are often considered viruses, viruses are only one form of malware, and not all types are viruses. A virus is a computer program that was originally written for entertainment but today mainly causes incalculable damage to information systems.

The term virus is used in computer jargon in the same way as self-replicating biological viruses – a virus is a program or code that automatically spreads to other files it encounters and performs malicious tasks, such as displaying simple message windows or destroying data. A virus can be described as a program that infects various media and changes the operation of a computer or network (Šepec, 2018). Or as a self-replicating program that can “infect” other programs by altering them or their environment, so that a call to the 'infected' program means a call to a possibly

modified and, in most cases, functionally similar copy of the virus (Horton & Seberry, 1997).

Viruses need user assistance to activate and spread, which happens when you click on a specific file, launch a specific program, or click on a link. When an infected file is opened, the virus spreads and can infect other programs, the boot sector of the hard disk, its partition, or a document. Once activated, it also starts spreading to other files or through other communication channels. A computer system can become infected even if the infected program is not launched, as some viruses spread while copying themselves. Viruses cannot infect a computer if we only view websites – infection occurs only if we allow online programs to run. It is good to know that viruses are not only present in stolen or cracked programs; due to carelessness, they can also appear in legal programs. Some viruses also spread via e-mail without attachments because of software errors (Šepec, 2018).

Viruses usually reside in individual executable programs on an infected computer, which increases the size of the program. The contents of the screen of the infected computer suddenly begin to change, individual parts of the screen may move, and various images or inscriptions may also appear, such as: "Your computer is now infected." The infected computer may request different passwords and codes or otherwise change typical commands sent via the keyboard or mouse. The computer's performance is also slowed down (this does not mean that every slow computer is also infected with a virus). Most viruses are designed to destroy the computer or data (Šepec, 2018).

Every virus has the following components (Šepec, 2018):

- infection: the part of the program that enables the virus to spread,
- payload: represents the main activity of the virus and is designed to perform specific functions, such as deleting, modifying and configuring data and installing software for remote access,
- trigger function: defines a time or event and executes a supporting component of the program.

3.1.2 Worms

Viruses differ from worms in that their launch requires action from the recipient in the form of program execution, with the user executing the virus file themselves (opening an email attachment, clicking on the executable file with the mouse). Worms exploit vulnerabilities in operating systems (for example: Windows and Linux) and do not require any action from the victim (Šepec, 2018).

Thus, a worm is an independent program that can spread copies of itself or parts of itself to other computers, usually over network connections, and these copies are fully functional independent programs that can either spread further and/or communicate with the parent worm (for example, to report the results of a calculation) (Horton & Seberry, 1997). They often attack important systems and websites. In the case of worms, the most noticeable consequence is increased network traffic.

Similar to viruses, worms are self-replicating programs that most often spread uncontrollably across a computer system, the Internet, and other networks (Šepec, 2018). However, compared to viruses, they are somewhat more intelligent, as they are able to automatically find suitable targets for infection and spread without user assistance, as they use errors in operating systems and programs (Bhargava et al., 2022). They are usually very successful in spreading, as computer users do not install the necessary security systems. Like viruses, worms carry a "payload" that allows them to control the infected computer, delete files, or steal personal information and data. In 2004, a worm called Blaster infected more than 100,000 computers in just five hours. Another worm, called Mydoom, is perhaps the worst malicious program in history, as it caused more than $38 billion in damage in 2004 (Paulo, 2022).

3.1.3 Trojan horse

A Trojan horse is incapable of self-replication. A characteristic of Trojan horses is that they often contain some innocent function (for example, displaying the time and weather on the desktop of a computer system) (Šepec, 2018), a small and harmful part of some original, generally useful program. Unlike a computer virus (which attaches itself to another program by any of a number of methods), a Trojan horse is a standalone program and may have user functions for the user (Horton & Seberry, 1997).

A Trojan horse can easily be presented as a seemingly innocent file downloaded from the Internet as a Word or PDF document attached to an email (Bhargava et al., 2022). When this generic program is installed, a Trojan horse is also installed with it, allowing the attacker to take over the computer. Although this type of malware does not replicate, it can perform several harmful activities. Behind the primary program are so-called "trap doors" that allow the author of the Trojan horse to perform a specific function (access the user's information system, retrieve files from the system, or install malicious code on the system). They work similarly to viruses, as they require some prior action from the victim in the form of running an executable file, visiting a website, or opening a seemingly innocent file containing the Trojan horse code. The main purpose of Trojan horses is to create and steal identities in connection with achieving financial gain (Šepec, 2018).

3.1.4 Spyware, adware and ransomware

Spyware and adware are major nuisances in the computer world. Both are types of malicious software and differ from viruses and worms in that they cannot spread from one computer system to another.

Spyware is a general term for various types of malicious software that controls the operation of information systems in a certain way and collects personal data (Šepec, 2018). It is a set of code that is installed on a computer system and acts as a spy, focusing on the activities of the system owner and collecting all information that it accesses without authorization (Maity & Dey, 2021). Spyware is installed on a computer while browsing the Internet and it exploits security flaws in the web browser to infect the computer. It can take various forms, from free programs, screen savers, to various toolbars, and even file sharing programs. One of the popular tricks of criminals is to redirect your browser to unwanted websites, which allows attackers to commit additional crimes. The purpose of spyware is not to destroy, damage or disrupt data and systems but to collect various information about the user (their habits and behavior, remembering and recording passwords and other confidential information) through websites, social networks and online stores, which is then reported back to a central source for either legal or illegal purposes (Šepec, 2018).

Adware collects data about users and their online habits and sends its findings to various agencies, which bombard users with ads and spam. Adware can constantly display pop-ups, which significantly slows down the computer (Šepec, 2018).

Ransomware is a self-explanatory term – programs hold critical information "hostage" to receive a ransom. The consequences can include data loss or unauthorized distribution of data to the public, affecting the future operations of an organization (Šepec, 2018), its reputation, or the reputation of an individual. Today, most ransomware occurs as a result of a computer worm that can spread from one system to the next and across networks without user intervention (Bhargava et al., 2022). Ransomware can target all industry sectors, with some more vulnerable than others. For example, in 2021, legal, manufacturing, financial, and human resources services (Cyberreason, 2022) were most affected by ransomware (Fedor, 2022).

3.1.5 Denial of Service

Denial of Service (hereinafter: DoS) is a type of cyberattack in which criminals make a specific network inaccessible to users and gain access to a computer system to collect personal information. The attack originates from a single system or network. It is an attempt by attackers to prevent a legitimate user of a service from using that service. A DoS attack can be carried out through (Šepec, 2018):

- disabling network routers that allow access to the Internet of the attacked information system. Wireless access points are reprogrammed to no longer provide a wireless Internet connection to the attacked IT systems,
- sending a mass of e-mail messages (mail bombing), which overloads the e-mail server,
- programs that constantly reproduce or other types of viral code that attack the information system.

Distributed Denial of Service (hereinafter: DDoS) is coordinated across multiple information systems, each sending a portion of the data to carry out the attack simultaneously from multiple attack points. It is a distributed denial of service of an information system. The attacker can attack multiple slave systems (slaves), which are controlled by control systems (masters). Attacks are often carried out on a significantly larger scale with multiple slave systems (Šepec, 2018).

4 Measures to protect against IT threats

The saying »prevention is better than cure« also applies when we talk about information and computer security. In today's highly digitalized and connected world, both individuals and companies are exposed to various dangers at every turn, which is why it is important to know how to protect ourselves from IT threats and malicious software. Various strategies and methods primarily follow the process of preventing, detecting or sensing and responding (Kemmerer, 2003) to IT threats. Cybersecurity is primarily concerned with protecting IT resources (information, applications or software, infrastructure, intangible assets and people) from unauthorized disclosure, modification or destruction. In this way, the IT requirements of the CIA triangle (availability, integrity and confidentiality) are ensured.

Information and computer security are key topics that need to be addressed and implemented in any company to ensure the protection of internal assets and intellectual property (McFadzean et al., 2011). Most companies (as well as individuals) operate online, as it enables real-time connectivity and communication (Chen et al., 2010). There are various ways in which a company can protect itself from IT threats and attacks. In certain cases, a financial investment is also required, which depends on the method and level of protection. First and foremost, it is necessary to educate and train people on appropriate behavior in cyberspace, since in most cases it is people who are responsible for the attack in the first place (opening inappropriate pages, clicking on web links or attachments). The subchapters cover some measures on how a company can protect its IT resources with the help of employees from IT threats and attacks. The same measures can also be used in the case of a physical individual to protect personal devices.

4.1 Creating passwords

Every user account and some applications require a password. Many people choose simple passwords, usually including their place of residence or birthplace, birthdays, children's or pets' names, and the like. Dictionary words are also often used in passwords. This is not a good idea, as they are easy to guess and relatively short. When attackers try to gain access to accounts, they use brute-force attacks, where they use software to "check" dictionaries and try a large number of different passwords, hoping that one of them will be correct (Kaspersky, 2023b).

The recommended password length is also being extended every year, with a minimum requirement of at least eight characters. Longer passwords are always better than short ones – the more characters there are, the longer it will take to "crack" the password or determine it. One additional character (letter, number or symbol) can extend the time to crack a password by months or even years. Therefore, it is always better to create passwords longer than the minimum required. It is recommended to use passwords with at least 12 characters. It is necessary to combine uppercase and lowercase letters, numbers and symbols. Of course, we must also pay attention to the order, as it is increasingly common for passwords to consist of (in this order): one uppercase letter, a set of lowercase letters, a set of numbers and one or two symbols. Therefore, the use of "salting and peppering" passwords is very important (The Upwork Team, 2021), which involves the random use of a mixture of uppercase and lowercase letters, numbers, and symbols, which greatly increases the level of difficulty and extends the time it takes to crack a password.

Due to overload, people tend to be lazy and overly-relaxed when creating online accounts, which is why we often use one password for multiple accounts, which is not recommended at all. When we use one password for multiple accounts or devices, attackers can access all these accounts and the data in them in the event of unauthorized access or hacking. However, if we have a different password for each account and device, only one account is at risk, and the others are not. This way, our data is more secure and protected from IT threats and attacks.

4.2 Computer network protection

Protecting IT infrastructure and applications or software, and consequently information and people in the company, can be achieved in various ways. Table 4.1 presents a set of preventive measures that a company can use to protect the aforementioned IT resources and their description.

Table 4.1: Preventive measures to protect against IT threats

Measure	Description
Installing IT security frameworks	IT security frameworks describe documented and mutually understood policies that dictate sensitive information management in an organization.
Creating a whitelist of applications	Based on the list of allowed applications, the company can determine which applications are allowed to be installed and/or run on company devices.

Measure	Description
Using antivirus software	It enables the maintenance of "clean" computers and operating systems by regularly checking, detecting, preventing and removing various malicious software.
Firewalls	A firewall sets rules that govern data traffic and controls the entry and exit of data and other devices into and out of the computer.
Using a network intrusion detection system (NIDS)	A network intrusion detection system (NIDS) works similarly to antivirus software and a firewall; it monitors traffic flowing into and out of various devices connected to the network and checks for malicious activities or unauthorized access and notifies the network owner.
Implementing multi-factor authentication	Information and data security can be ensured based on multi-level authentication, required for access to sensitive information. In this case, it can be a combination of entering different passwords received via different devices (phone and computer) or accounts (email, phone number).
Using encryption	Asymmetric encryption protects sensitive information that is transmitted from one device to another, either over the Internet or other devices. A document or file is encrypted (created as ciphertext) using a public key and then decrypted (changed back to plaintext) using a private key.
Using a virtual private network (VPN)	A virtual private network (VPN) is a way to create a private place on the Internet that helps users create a secure connection and encrypt data sent over the network. VPN is often included in antivirus software.
Using honeypots	"Honeypots" are artificially created targets that contain useless information. While attackers unknowingly try to access honeypots, important information and files on the computer are protected.
Performing a vulnerability assessment and penetration test	Performing a vulnerability assessment involves looking for potential problems in a network or system that could allow unauthorized external access. Vulnerabilities are discovered and their severity is determined with priority for resolution. The latter is done by attempting to access the network or system from the outside, with the help of ethical hackers.

Source: (Chen et al., 2010; The Upwork Team, 2021; Vacca, 2013)

5 Conclusion

In 2020, an average of 360,000 new malicious files were discovered (Kaspersky, 2023a), and every year their authors become more innovative. New types of malicious code are emerging that can exploit security vulnerabilities in operating systems, antivirus programs and firewalls. The most common malicious codes that dominate criminal acts, in which various methods are implemented, are disruption, damage and severe obstruction of information systems and electronic data (Šepec, 2018).

The Internet has become the most common place for viruses to spread. Malicious software can be hidden in anything downloaded from websites, and without a proper security system, it can cause a lot of damage. Due to the rapid growth of email, attachments have become the most common reason for the spread of computer

viruses. It is important to note that there are many different types of malware, which are improving, multiplying, and appearing in new forms or variations almost every day.

Therefore, information and computer security of companies must also include protection against social engineering, such as various forms of phishing (including smishing and vishing), as attackers often target the human factor as the weakest link in the security chain. Phishing attacks, where attackers pose as trusted entities to obtain sensitive data or access to systems, are particularly dangerous in logistics due to the complex and branched supply chains. Employees may receive fake emails urging them to reveal passwords, credit card numbers or other confidential company information, which can lead to serious security incidents and business disruption. Therefore, it is crucial that companies conduct regular training and awareness-raising among employees on how to recognize phishing attempts and implement security measures that reduce the risk of such attacks.

In the context of the digitalization of logistics, information and computer security play a key role in ensuring the smooth and secure operation of logistics processes. Digitalization brings many benefits, such as increased efficiency, better traceability of shipments and optimization of inventories, but at the same time it exposes companies to IT threats and attacks. Cyberattacks such as system intrusion, data theft or ransomware attacks can cause serious disruption in supply chains, leading to delays, financial losses, and general damage to the reputation of companies. Therefore, it is imperative that companies invest in information and computer security through the appropriate solutions and measures presented within this chapter.

Information security in logistics, in addition to the above, also refers to the protection of confidential data, such as information about customers, transactions, suppliers and business partners, and others. Effective data management is essential for maintaining trust between business partners and end users. Compliance with legislation and data protection standards, such as GDPR and ISO 27001, is an important aspect of information security, ensuring that companies operate in accordance with legal requirements and best practices. Security policies and procedures, including regular security reviews and risk assessments, are essential in preventing security incidents and mitigating risks in the digitalization of logistics.

References

Bhargava, P., Choudhary, R., & Gupta, A. (2022, May). A Review Study on Computer Virus. *World Journal of Research and Review (WJRR)*, *14*(5), 39–44.

Chen, R.-S., Chung, Y.-M., & Tsai, C.-H. (2010). A study of the performance evaluation of a network intrusion detection system. *Asian Journal on Quality*, *11*(1), 28–38. https://doi.org/10.1108/15982681011051804

Cyberreason. (2022). *Ransomware: The True Cost to Business—A Global Study on Ransomware Business Impact*. https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf

Fedor, O. (2022, November 3). *93 Must-Know Ransomware Statistics [2023]*. Antivirus Guide. https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=Cj0KCQjwi46iBhDyARIsAE3nVrYtrwBey_1ErcYLO6UBJVk3as7CfdxsGKVcHVkKJfM_Mcyvk92IlH0aAr3WEALw_wcB

Horton, J., & Seberry, J. (1997). *Computer Viruses—An Introduction. 19, 1*, 122–131. https://documents.uow.edu.au/~jennie/WEBPDF/1997_09.pdf

IBM. (n.d.). *What is a mainframe?* IBM. Retrieved 4 October 2023, from https://www.ibm.com/topics/mainframe

Information Security: The Ultimate Guide. (n.d.). *Imperva*. Retrieved 3 October 2023, from https://www.imperva.com/learn/data-security/information-security-infosec/

IT Governance Institute. (2007). *COBIT 4.1: Framework, control objectives, management guidelines, maturity models*. IT Governance Institute.

Jereb, B. (2017). Mastering logistics investment management. *Transformations in Business and Economics*, *16*, 100–120.

Jereb, B., Cvahte Ojsteršek, T., & Rosi, B. (2016). *Governance of Investments in Logistics* (pp. 236–247). https://doi.org/10.4018/978-1-5225-0001-8.ch011

Kabanda, G. (2019). *Trends in Information Technology Management*.

Kajba, M., & Jereb, B. (2021). *Three Crucial Years of IT Trends in Logistics*. 187–198. https://www.elibrary.ru/item.asp?id=46600879&pff=1

Kajba, M., Jereb, B., & Obrecht, M. (2023). Considering IT Trends for Modelling Investments in Supply Chains by Prioritising Digital Twins. *Processes*, *11*(1), Article 1. https://doi.org/10.3390/pr11010262

Kaspersky. (2023a, May 18). *The number of new malicious files detected every day increases by 5.2% to 360,000 in 2020*. Www.Kaspersky.Com. https://www.kaspersky.com/about/press-releases/2020_the-number-of-new-malicious-files-detected-every-day-increases-by-52-to-360000-in-2020

Kaspersky. (2023b, June 30). *Brute Force Attack: Definition and Examples*. Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.*, 705–715. https://doi.org/10.1109/ICSE.2003.1201257

Maity, S., & Dey, D. (2021). Computer Virus Attacks. *La Pensée*, *51*(3), 585–594. https://doi.org/10.6084/m9.figshare.19258763.v1

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2011). Information Assurance and Corporate Strategy: A Delphi Study of Choices, Challenges, and Developments for the Future. *Information Systems Management*, *28*(2), 102–129. https://doi.org/10.1080/10580530.2011.562127

Paulo. (2022, December 21). *Top 10 most dangerous computer viruses of all time*. Dynamic Solutions Group. https://www.dsolutionsgroup.com/top-10-most-dangerous-malware-of-all-time/

Šepec, M. (2018). Kibernetski kriminal: Kazniva dejanja in kazenskopravna analiza. In *Univerzitetna založba Univerze v Mariboru*. Univerzitetna založba Univerze v Mariboru. https://press.um.si/index.php/ump/catalog/book/335

The Upwork Team. (2021, June 8). *What Is IT Security? Examples and Best Practices for 2024*. https://www.upwork.com/resources/it-security

Vacca, J. R. (2013). *Cyber Security and IT Infrastructure Protection*. Syngress.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

What Is Computer Security? (And Why It's Important). (2022, August 23). *Berkeley Boot Camps*. https://bootcamp.berkeley.edu/blog/what-is-computer-security/

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (4th edition). http://almuhammadi.com/sultan/sec_books/Whitman.pdf