Information Security Management in Organisational Settings and Higher Education Institutions

Kaja Prislan
University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
kaja.prislan@um.si

Abstract In modern times, marked by trends in digitalisation, e-commerce, and the use of advanced technological solutions on the one hand and increasingly common and dangerous information threats on the other, information security management and information incident prevention have become crucial for successful and efficient organisational performance. This chapter presents the basic concepts and approaches to information security management in organisational settings and the core factors and contemporary trends that affect information security risks. Special emphasis is placed on the review of information security in higher education institutions, which are particularly exposed to cyberthreats due to their specific activities, culture, and values.

Keywords: information security, information risk, management, organisations, higher education institutions

University of Maribor Press

DOI https://doi.org/10.18690/um.1.2023.1
ISBN 978-961-286-693-8

1 Introduction

Digitalisation, e-commerce and communication, and the development of advanced technological solutions, belong among the most actual trends of modern times, causing drastic changes in the security field at the same time. Although the performance of various activities has been simplified and enhanced (as there are communication, socialisation, learning, data management, business and decision-making), there is also the phenomenon of new security risks.

The main side-effect of technological development and progress are information threats and cybercrime, strongly influencing changes in traditional pre-conditions for providing security and privacy. In the 21st Century, threats of that kind gained unimaginable dimensions. Cyberthreats representing a rarity a decade ago, are a daily thing in contemporary times. At the same time, they constantly develop further and become more and more organised, sophisticated and unpredictable. A challenge exists mainly because such crimes do not know for geographical or other borders and cause severe damage to individuals, as well as to organisations and countries throughout the world.[1] Due to the hidden nature of actions by criminals, cyberthreats are difficult to recognise, as they might perform undiscovered in a system (or abuse a system and its data, respectively) for a longer time. At a particular moment, they might disable critical processes and systems. Due to its unpredictable and hardly manageable nature, cybercrime has become the main security problem of contemporary times (*EU Security Union Strategy, 2020; Interpol, 2021*). In line with growing threats caused by cybercrime and threats connected to privacy and personal data protection, in 2020, a new *EU Cybersecurity Strategy for the Digital Decade* was adopted. In the strategy, as one of the key challenges of the EU, a lack of collective awareness of cyberthreats is stressed, and among the goals belong efforts to establish joint capacities for reaction to cyberattacks, development of organisational capacities and technical protection as well as regulation of behaviour and privacy in the internet.

[1] According to assessments of security organisations, cyber-crime causes a damage of approximately six billion dollars or more than five billion Euros on an annual base (Morgan, 2020; The EU's Cybersecurity Strategy for the Digital Decade, 2020), while interferences into political processes are threatening also the pillars of democracy (Laţici, 2019).

Most negative effects of digitalisation and technological development are faced mainly by organisations and subjects of commerce (European Crime Prevention Network, 2016). The newest data show that in Europe, each eighth enterprise has been a victim of a cyberattack already (Eurostat, 2020), and there are multiple reasons for that. Organisations support their success or development, respectively, with different technological solutions that have a double role in the commercial surrounding; they are a source of competitiveness and numerous security vulnerabilities. In the same way, organisations managing a growing number of data is the primary goal of committers of cybercrime. Namely, in the world of commerce, information is the most important capital and source of power and, consequently also a very much searched good (Furnell & Moore, 2014). The main advantage of information and communication technology [ICT] and information systems for organisations lies within the improvement of the effectiveness of commerce and decision-making, but because information systems save vast amounts of personal data and other relevant information (e. g. intellectual property and business secrets) they also became exposed and when protected the most vulnerable point in an organisation's structure insufficiently, because of numerous vulnerabilities and simple possibilities of abuse.

Therefore , the concept of organisational security has strongly changed by moving organisations into cyberspace. Compared to other forms of threats, information or cyberthreats create specific risks, because of which the system of organisational security gained a new dimension. Information systems created a unique environment within an organisation composed of its most valuable assets. At the same time, they created a new entry point into the organisational structure, through which all other physical and technical security measures may be circumvented. When organisational security could be taken care of only by technical and physical protection are over (Prislan & Bernik, 2019).

Numerous well-known cases of hacker attacks, intrusions into information systems, identity thefts, disclosure of personal data, espionage and trade with business secrets that we witnessed in the past years prove that the stability and success of commerce in the information era is strongly depending on the capability to manage information security risks and to provide for information security. Although practically every organisation may be the target or victim of an information incident, certain branches (e. g., health, finances, production, high-tech, education, governments, energy or

critical infrastructure) are stronger exposed to such kinds of risks due to their sensibility and number of confidential data managed by them.

Providing information security represents a substantial managerial challenge. Despite the negative influence of information incidents on organisational security, systematic and strategic management of this field is merely in a developmental phase in many organisations. Recently, progress and development were to be noted in the field of organisational practice, but threats develop essentially faster than organisations can follow. A major challenge lies within the fact that information security is a complex system to be handled by a plan systematically on a multilayer and multidimensional level.

This chapter aims to present basic concepts of information security management, i. e., key aspects and steps relevant to the establishment of a successful approach to providing information security in organisations, and actual trends in the field of cyberthreats and information security risks. There, special emphasis is placed on the state and management of information security in higher education institutions. Namely, the education branch, due to its nature and culture and growing digitalisation and distance education, in the scope of cybercrime and information threats, belongs among the most exposed and vulnerable branches (Alexei, 2021; Check Point, 2022).

2 Development of the Information Security Discipline

The vast expert discussions and research activity of the past two decades led to a better understanding of the complex nature of information security and the development of scientific cognitions in this discipline. Approaches to providing information security developed parallel to the development of ICT, but views on the security of information systems were oriented towards technical aspects and mechanisms at the beginning (Whitman in Mattord, 2012; Von Solms, 2010). Due to this, the development of information security discipline ran slower than the development of threats and crimes in this field in practice.

Due to expert assessments, information security as a discipline started to develop intensively after the year 2000. Till the middle of the 90s of the past century, mainly IT experts dealt with such aspects, and attention was directed towards basic technical protection. Later, views on security and privacy changed or were upgraded; respectively, information security exceeded traditional frames and gained the mark of an interdisciplinary science (Anderson & Moore, 2009; Hommel, Metzger, & Steinke, 2015).

Development of information security through time may be comprised of five larger periods that differ regarding the aspects that were developed in that time and were exposed as a priority in the providing security of information and information systems (von Solms, 2010). The first period is called the *technical wave*, which lasted till the 80s of the past century. In this period, simple technical measures were developed (e. g., identification and authentication procedures), and questions of security were usually dealt with by technicians or computer experts, respectively. The second period or the so-called *management wave* ran till the middle of the 90s. During this time, policies intensively started to develop, procedures were prescribed, special organisational departments were established, and specific responsibilities for information security were trusted to managers or the leadership level. The reason laid within the phenomenon of a growing number of interconnected technologies in networks and the distribution of data. The *institutional wave,* or the third period, lasted till about the year 2005. This period was marked by the cognition those information threats may have severe consequences for organisations. By this, the convincement prevailed that the approach to providing information security has to be inter- and multidisciplinary. Information security has become increasingly the responsibility of strategic management and an important part of organisational culture. For the fourth period, named the *information security governance wave* that started in 2005, the development of different standards and stronger warnings to the management to take responsibility for the management of information security risks is characteristic. By 2006, almost parallel to the fourth period, the fifth period or the so-called *cybersecurity wave,* started. After this milestone, concepts of protection and management were upgraded as a consequence of a growing inclusion of organisation in cyberspace, a growing digitalisation and the phenomenon of more and more organised and sophisticated threats and attacks.

Based on the development of cognitions and different views on the nature of information security and information threats, also definitions of information security gradually developed. Today, the most frequent and established definition used by different international and expert organisations is that information security refers to the protection of information and information systems from unauthorised access, use, disclosure, defect, change or destruction with the aim of guaranteeing its *confidentiality, integrity and availability*. (ISO/IEC 27000:2018; Nieles et al., 2017). Thus, it is about a system of security or protective measures and mechanisms to provide for three intervening target states formed by the so-called *CLA triad* – a model of attributes of information security established in the field (*confidentiality, integrity, availability*).

For confidential, personal data and information with a high value, confidentiality is an extraordinarily relevant security aspect. Providing for confidentiality refers to the prevention of unauthorised disclosure of information. The condition of confidentiality is met when information is protected from disclosure or unauthorised insight, and only users with proper access rights with a purpose have access. Confidentiality is connected to the concept of mystery and privacy, meaning that information remains hidden or covered and inaccessible for all people and services without being granted access. The most frequent measures of providing confidentiality are encryption or coding of data and communication, security classification of information, systems of registration and prevention of intrusion (IDS/IPS), antivirus programmes, management with access and user rights, the definition of responsible persons and their responsibilities as well as awareness of users on legitimate use (Osborne, 2006; Pfleeger & Pflegger, 2006; Seese, 2009; Whitman & Mattord, 2012).

The criterion of *integrity* refers to the providing for quality of information. This means that information can be trusted or was changed or processed only by authorised persons. Consequences of loss of integrity are incorrect, false or unreliable information that may lead to wrong decisions. Providing for integrity includes verifying credibility and protecting information from unallowed changes and their integrity. The main measures fitting this criterion are following the revision trail, access control, user rights management, verification of thickening value and trust-building (Boersma, Loke, Petkova, Sander, & Brombacher, 2004; Osborne, 2006; Pesante, 2008; Pfleeger & Pflegger, 2006; Whitman & Mattord, 2012).

Availability is a condition meaning that information and systems are available whenever authorised users need them. The main characteristics of availability are system accessibility, reliability and appropriate permeability of a system (*ISO/IEC 27000:2018*; Nieles et al., 2017). Availability is tightly connected to the reliability of the functioning and capacity of information systems, and measures attempt to prevent loss of information, defects, unavailability or degradation of information systems. Among the most frequent measures of providing for availability belong antivirus programmes, security copies, doubling critical parts of information systems, use of reliable infrastructure and proper maintenance, network surveillance, systems for detection and prevention of intrusion (IDS/IPS), reaction plans for incidents and resilience (Nieles, Dempsey, & Pillitteri, 2017; Osborne, 2006; Pesante, 2008; Whitman & Mattord, 2012).

By the described attributes or criteria of information security, some other phenomena relevant to be respected and achieved in a system of information security are connected. These are (Whitman & Mattord, 2012): (a) accuracy connected to integrity and referring to reliability and flawlessness of information and guarantee for an expected value; (b) authenticity likely connected to integrity, but referring to quality and legitimacy, which means that data are authentic, original and trustworthy or do not contain harmful elements; (c) utility connected to availability, but meaning that data is properly formatted, presented or saved and have a value for use at work or decision-making to the user; (d) possession is connected to the criterion of confidentiality and refers to the request that the use of a system and data processing is controlled by owners or caretakers with the intension to provide for proper supervision, overview and traceability of activities and events of information use. Also, Ulven & Wangen (2021) state in a similar context that the CIA triad has to be upgraded, i. e. by concepts, as there are: privacy, identification, authentication, authorisation and accountability.

Thus, today information security is not just a technical question, but a complex, multidimensional field composed of a *social and technical sub-system*. This means that information security is influenced by organisational, human, as well as by technological factors (Prislan, Mihelič, & Bernik, 2020). When planning the mere approach and measures, besides the described attributes or criteria, organisations must understand the role or function of information security in the organisational environment, as well. A relevant role of information security is providing for an

uninterrupted activity (i. e., providing for the capability of uninterrupted functioning of information systems despite a potential event and incident) and *information security risk management* (i. e. providing for a state of acceptable risks or minimum risk). Despite the importance of information security for commercial success, in the building of this, one must also respect the needs for rationality, economy and flexibility. Namely, it is impossible to provide absolute security, as all risks cannot be predicted or even addressed in a meaningful way.

3 Relevance of Information Security in the Organisational Context

In practice, within organisations, there are frequently questions regarding the relevance of information security and the need for investment in the mentioned field. The reason for this is a lack of tangible profitability of investments in information security, as security measures are aiming at a reduction of losses and not at common creation of profit (Schatz & Bashroush, 2017). Since security is a field without direct financial income, sceptical views on investments are not rare. In the same way, among the leadership of an organisation, too optimistic or indifferent views on information security risks and threats as well as one own vulnerability or exposition, frequently come up. Consequently, information security, in many cases, is understood as an unnecessary cost and as a function demanding too many means (Igor Bernik & Prislan, 2016). To overcome the wrong convictions, an understanding of the implications of risks and actual input from information security to commercial or organisational success must be provided for on the leadership levels.

The relevance of information security for organisations may be seen similarly to the commercial value of ICT and information systems. Commercial value of ICT is provided for when it contributes to a higher effectiveness of commerce and a higher competitiveness of an organisation (Melville, Kraemer, & Gurbaxani, 2004). Departing from such a view, the added value of information security is reached when expected positive effects and influence on the conduction of commercial processes are reached.

With a proper approach to management, information security may have numerous short-term and immediate, as well as long-term and mediate effects. *Immediate* or *operative effects* are visible in a more effective conduction of processes and commerce, as through the definition of accountability, reduction of incidents and better reaction to events, a contribution to lower interruptions, quicker reactions, a higher situational awareness, better surveillance and consequently lower costs connected to security incidents is made. Mid-term and long-term effects give *tactical* and *strategic advantages* to organisations. Effects of a strong and qualitative information security are seen in improved relations with partners, a higher compliance, positive external audits, a higher level of trust or legitimacy and reputation in the public (Enzingeard et al., 2005; Wlosinski, 2019). A high integrity, trust and a positive public image belong among the main long-term effects of information security. Implications of this kind may contribute to a higher market value of the enterprise and commercial advantages on the market. Namely, showing a high responsibility in providing for information security frequently is a pre-condition for entrance into commercial connections, partnerships and acquisition of new business, mainly in the international context (BSI, 2018; Ezingeard, McFadzean, & Birchall, 2005).

In the opposite case, when organisations do not invest in information security development and management, the implications of the success and reputation of organisations may be extraordinarily negative. The consequences of realised information security incidents may be divided into financial or immediate and mediate or long-term consequences. *Financial consequences* most frequently show in the form of damage appearing from cancellations and interruptions of work processes or in a lower sale of services and products. Besides, among immediate costs also belong financial sources needed for recovery and healing from the consequences. One must respect that abuse or loss of personal data or data on foreign property leads to civil legal claims or criminal accusations. Besides financial consequences, information security incidents may also have *other negative effects* that are harder to measure but may have even worse consequences. They influence immaterial assets and refer e.g., to loss or decrease of reputation in the commercial environment and on the market. In case of a bad information incident, an organisation may become a target of attention from the media, influencing the opinion and convictions of clients and/or business partners and may contribute to a loss or decrease of commerce. Potentially, public accusations and decrease of credibility may follow. At the same time, also the competitive advantage may be

endangered, when intellectual property and business secrets are stolen or alienated (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018; I. Bernik, 2014; EDUCAUSE, 2019a; Prislan & Bernik, 2019; Tayaksi, Ada, Kazancoglu, & Sagnak, 2021).

Besides all mentioned advantages and positive effects of information security on the commercial success of an organisation, mainly its contribution to business continuity and compliance is of key importance.

Business continuity generally refers to the capability of an organisation to maintain and tackle unpredicted events successfully. This means that the organisation can survive unpleasant situations – it is able to do business or resurrect its processes and continue business in spite of catastrophes, incidents or environmental influences. A composite part of this is the preservation of functioning and renewal of key business processes. Business continuity is a part of strategic management and, in modern organisations, includes reactive (plans and processes for recovery) as well as proactive (plans and processes for resilience) functioning. There, information security is merely one of the fields contributing to providing for business continuity, as unpredicted events may be connected to most various risks, and it is a fact that threats and incidents in connection to technological development and progress of an organisation strongly threaten the capacity of business continuity (Niemimaa, Järveläinen, Heikkilä, & Heikkilä, 2019).

Compliance is one of the pre-conditions to be met by an organisation, as by this, they meet the demands for legal and legitimate business. Providing for compliance is connected to various fields, and it is especially relevant in the context of information security, where prescribed demands regarding privacy, personal data protection and information system security must be met. Within information security, in the first place, it refers to respect for legal regulations and the conduction of measures within their framework. Information security must be regulated in a way prescribed by legislation – in the management, processing and protection of data and information systems, prescribed measures are taken, and at the same time, no exaggerated or disproportional control is carried out. This means that the rights of those who are object to security measures, e.g., the data and system users, are respected. Organisations must know all key legal acts referring to their business and security and must take care of meeting these demands by proper measures. Disregarding the

kind and structure of an organisation, meeting legal provisions is obligatory, else prescribed accountability is violated, and legal consequences might follow. Besides a legal compliance, there are also other aspects of compliance referring to respect and following of internal acts, contractual obligations and other professional and international directives or good practices. Thus, compliance as field of information security implies the following aspects: compliance with (national and international) legislation; compliance with the organisational strategy and internal rules and instructions; compliance with obligations departing from contracts, and agreements; compliance with standards and recommendations in the field of information security; and compliance with (national, international) strategies (Prislan & Bernik, 2019).

4 Approach to providing form Information Security

To increase of complexity of information systems and information security risks in organisational environments, among experts, a position has been established that information security must develop as a business function and special organisational activity (Baskerville, Spagnoletti, & Kim, 2014; Bojanc & Jerman-Blažič, 2008; Chang & Ho, 2006; Feng, Wang, & Li, 2014; Mishra & Chasalow, 2011; Thomson & von Solms, 2006), and in management an interdisciplinary and team approach is necessary. Everybody responsible and competent to provide for information security in an organisational environment must be aware that information security is not just a matter of a purchased technical product or exclusive responsibility of the IT department, but a matter of the whole organisation, as the leader as well as each employee, as it is them, who take care that the definitions of rules become alive in practice (Prislan & Bernik, 2019).

Accountability for providing information security lies in the hands of three groups inside an organisation, as there are: *owners* of information sources (are owners of information and accountable for the definition of their confidentiality); *custodians* of information sources (are defined by the owners and accountable for operative conduction of measures and rules of information security, surveillance of the state and reporting to owners); *users* (the use information sources at work and are accountable for respecting the information security rules and policies) (Whitman & Mattord, 2012). Concretely, basic accountability is divided between the top and the operative management, among the main work spaces having determining functions

or being connected to information security management, belong: CEO (*Chief Executive Officer*), CIO (*Chief Information Officer*), SAISO or CISO (*Senior Agency Information Security Officer* or *Chief Information Security Officer*), AO (*Authorizing Official*), SAOP (*Senior Agency Official for Privacy*), SSO (*System Security Officer*), ISA (*Information Security Architect*), SSE (*System Security Engineer*), SCA (*Security Control Assessor*) and SA (*System Administrator*). Among support personnel cooperating in the management process belong the responsible staff for fields as there are: physical security, audit, quality, personnel, crisis management, privacy, and similar. There, such detailed division of staff usually is characteristic for larger organisations, whereas in smaller organisations, they usually might be united (Nieles et al., 2017). In discussions on the way of organising and placing information security functions (and personnel) in a hierarchic structure, the importance of providing for a direct communication/report line of accountable staff towards the leadership level and the best possible (financial, decision-making, personnel) independence of this function is stressed (Goodyear, Portillo, Goerdel, & Williams, 2010; Klimoski, 2016).

In line with the complex nature of information security in organisations, it is frequently compared to a puzzle – it is composed of multiple parts that must be compliant and connected. Here, the authors define different fields and dimensions of information security; some of them are presented below.

De Oliveira Albuquerque, Villalba, Orozco, Buiati, & Kim (2014) describe the TISA (*Trust Information Security Architecture*) model, where four fields of information security and measures connected to it are defined. The *first field* encompasses planning of measures and includes activities in connection to the identification and assessment of confidentiality of information systems and information sources, providing for their integrity, confidentiality and availability, management of digital identities, access control, cryptographic data protection, and protection of privacy and anonymity. The *second field* encompasses the definition of rules, which includes adopting an information security policy. The *third field* includes the conduction of operational activities and mainly refers to the surveillance of processes and respect for rules, the performance of audits and supervision of information security risks. The last and *fourth field* intervening with the other three refers to trust-building, where it is about strengthening legitimacy, compliance and verification of integrity with the purpose of building a system, where expectations as well as goals are met.

Von Solms (2001) as an example mentions 12 different dimensions that together form a system of information security: the *strategic dimension* includes activities connected to planning and support; the *organisational dimension* 8includes processes connected to management; the *political dimension* includes activities connected to definition of information security strategy and policies; the *ethical dimension* refers to transparent decision-making and conduction of measures; the *certification dimension* refers to processes of accreditation; the *legislative dimension* refers to providing for compliance; the *insurance dimension* encompasses insurance for cases of information incidents; the *personnel dimension* refers to processes and measures connected to users; the *cultural dimension* includes development of a security culture; the *technical dimension* refers to planning and conduction of technical measures; the *evaluation and audit dimension* includes processes connected to assessment of effectiveness, audits and controlling.

Similar descriptions come from Hagen, Albrechtsen, & Hovden (2008), who connect effective information security to four intertwined fields: the *management perspective* refers to processes of information security risk management; the *economic perspective* includes demands for economic and rational investments; the *normative perspective* includes providing for compliance, the *cultural perspective* refers to the development of security culture and awareness.

According to the variety of fields forming an information security system and heterogenous factors influencing the state of information security, decisions of management must be based on an analytical or systematic process. In this process, organisations must manage and master information security risks: this means that they must periodically analyse the actual state of security and risks and, based on the cognitions, take decisions on proper ways to provide information security. Such an approach is comprised of an information security system described in detail below.

4.1 ISMS and Information Security Risk Analysis

ISMS (*Information Security Management System*) is an array of measures, procedures and policies for systematic data security management in an organisation. The goal of such a system is pro-active addressing of information security risks and decrease of effects by eventual incidents.

The model or framework of ISMS is defined in the international standard ISO/IEC 27001. The latter describes a model of composition, maintenance or preservation, surveillance, and improvement of ISMS, while directives and controls for meeting the pre-conditions and demands from ISO/IEC 27001 are presented more detailed in the standard ISO/IEC 27002. The mentioned standards are a part of the family or series of standards ISO 27000, addressing various aspects of information security management.

The range and contents of ISMS must respect organisational specifics, and therefore standards for building the system are relatively flexible and adaptable (in case that the organisation wishes to be certified according to the standard, certain demands and pre-conditions are obligatory to be met, others are optional). Building and introduction of ISMS in a certain organisation is influenced by its goals, vision, security requests, processes, size, and organisational structure. The influence and running of ISMS are mostly influenced by security requests depending on the nature of the commercial branch, form of business and commercial processes, technologies, connected subjects (partners, suppliers, and similar) and information security risks faced by the organisation.

The building and maintenance process of ISMS is based on the PDCA (*Plan, Do, Check, Act*) model. From this point of view, ISMS is a circular process that must be constantly assessed, supervised and updated after planning and building, what means that the process really does never end. Below (table 1) activities within each individual phase of building ISMS in line with the steps defined in the PDCA model are described in more detail.

Presented levels of ISMS and individual activities represent a systematic approach to information security regulation. Regarding the needs, an organisation may widen individual phases (e. g., the establishment of compliance may be a separate process/project), and opposite to this, individual phases may be joined. Due to the flexibility of the model, organisations may introduce ISMS into their own structure in different ways.

Table 1: Building ISMS in line with PDCA model

Phase	Activities
Plan. **Start of ISMS**	– Decision on introduction and way of introduction – Definition of range and limits of ISMS – Definition of approach to risk assessment – List of information – Status analysis – Validation and risk assessment – Analysis of possibilities of risk handling – Selection of control – Plan of handling – Obtaining approval from leadership – Assessment of compliance with legislation
Do. **Introduction and Performance of ISMS**	– Implementation of plan for risk handling – Implementation of control – Definition of methodology for assessment of effectivity – Implementation of training and education programmes – Means management – Implementation of measures for incident recognition
Check. **Surveillance and control of ISMS**	– Surveillance and control, failure discovery – Regular analysis of effectiveness of control, measures and processes – Risk control and surveillance – Leadership controls – Addition to plan, policies, ISMS documentation – Notification of events that may influence security and effectiveness
Act. **Maintenance and Improvement of ISMS**	– Correctional and preventive measures based on established lacks in the past step – Reporting – Follow-up on corrections

Information (Security) Risk Management is a composite and key part of providing information security. It is about a process, where it is established, what risks threaten an organisation, what are more or less frequent/dangerous and how to prepare for them. After the definition, an *information security risk represents a probability that an unpleasant event or incident will happen.* As mentioned, it is not a goal to provide for total security, and therefore in the process of risk analysis, it must be established, what risks are most dangerous and probable. For the calculation of risk or probability, a threat assessment, an assessment of vulnerability and an assessment of consequences are needed. Thus, *information security risk analysis* is a composite part of the information risk management process that is a process of assessing the organisational state in a quantitative form. Like the building of ISMS, also in information security risk

management, it is important to conduct the process constantly (periodically) and systematically throughout individual phases and steps that might be joined or widened for practicality and rationality. Thus, in the process of information security risk analysis, the needs of organisations are established, and responses to relevant questions are received (*ISO/IEC 27005:2018*), as there are: *why we need protection, what are we going to protect against whom or what are we going to protect ourselves and how are we going to regulate protection.*

Basically, the process of information security risk analysis is divided into three main phases (ENISA, 2015; Whitman & Mattord, 2012):

1. *Identification:*

- Identification (listing), classification, and prioritisation of information and information sources
- Identification, prioritisation, and assessment of information threats
- Identification of information vulnerability

2. *Assessment:*

- Determination of methodology
- Risk calculation

3. *Control:*

- Determination of acceptable risks
- Selection of strategy for handling risks
- Assessment of benefits and feasibility of the strategy
- Argumentation for the decision and reporting to interest groups
- Implementation, control or surveillance and maintenance of measures.

When selecting the approach, the organisation defines the range of the analysis and builds a plan; then it conducts the analysis of all major elements, makes the calculation and takes a decision on how to handle the risks. Here, various possible decisions are at hand, as there are: *acceptance of risks* – no reaction; a *decrease of risks* –

reactive measures; *mastering risks* – preventive measures; *avoiding risks* – getting rid of or dropping of elements creating vulnerability; *risk transfer* – transfer of accountability to a third subject. If the organisation decides to take measures, various security measures are at hand for this purpose.

Through similar steps, the risk management process is also defined by the standard *ISO/IEC 27005: 2018*. Regarding the directives by the standard, the mentioned process runs through five phases: (a) determination of a reference framework for analysis; (b) risk assessment; (c) decision-making regarding risk handling; (d) notification of interest groups; and (e) follow-up, surveillance, verification and updating of measures.

For easier planning and conducting of the described process, besides orientations contained in different standards and directives (e. g. ISO/IEC 27005, BSI 100-3), organisations also have more practical models at hand, as well, e. g. OCTAVE, MEHARI or MAGERIT models (Hommel et al., 2015).

4.2 Information Security Risks, Threats, Vulnerabilities and Measures

Situations threatening the state of information security differ by intensiveness and degree. Generally, potentially dangerous situations categorise as a security event (phenomenon representing a deviation from the normal state or having a potential threat to information security) or security incident (an event likely to threaten business and data security) (ISO/IEC 27000: 2018, 2018), and the way of response and measures depends on the classification,

An information event is a deviating phenomenon in the use of data or an information system representing some unpleasant situation of state of potential danger, but not necessarily leading to damage. An *information incident* is a real danger for the organisation and the state, where measures must be taken (Nieles et al., 2017). Organisations must be well-prepared for incidents, and they have to place attention also on other events, as by false handling, they might grow into an information incident. Events and incidents realise when a vulnerability used by the threats is present in the security system.

Thus, information security risks lead to unpleasant phenomena influencing or threatening the state confidentiality, integrity or availability of information systems and data. Key elements of information security risks are *information sources, information threats, information vulnerabilities and information security measures* (*ISO/IEC 15408-1:2009*). When vulnerabilities appear on a certain information source level, there is a potential danger that an (intentional or unintentional) threat using vulnerability with a certain technique might become a reality. Whether the threat will become a reality and lead to an incident or not is depending on the measures protecting the sources or decreasing vulnerabilities.

Information sources are data and information capital owned (or managed and processed) by an organisation. Among the most relevant data managed by organisations belong personal data, financial data, secret data, business secrets, intellectual property, data of business partners or connected subjects, passwords and data in connection to digital identities as well as services of trust and other data relevant for development and competitiveness of an organisation (e. g., strategic and development plans). Data must be protected and secured in all phases of management (establishment, processing, saving and transfer), disregarding their (digital or physical) form. As data are managed with the help of information systems, among relevant elements to which threats and vulnerabilities are connected belong also to other components of organisational information systems (technologies (software, hardware, networks, mobile tools, etc.), people and processes). Here, actual reports (Verizon, 2021) show that among the most targeted data of cyberattacks belong passwords, usernames, personal data, health and bank data.

Information threats are situations or phenomena that may use vulnerability on the level of information systems and, by this threaten confidentiality, integrity or availability of data and lead to an information event or incident. Information threats may be intentional or vicious, or unintentional. The first group is most frequently connected to planned vicious actions by (external and internal) individuals, organisations or other groups who want to use or harm an organisation. In this case, it is about the so-called cybercrime.[2] Among these, mainly financial and also espionage motives

[2] An international definition of forms of cybercrime was given by the Council of Europe in the (*Convention on Cybercrime*, 2001)[2], where five kinds of criminal acts were defined:

- crimes against confidentiality, integrity and availability of computer data and systems (illegal access, interception, disturbance and abuse of data, systems and installations),

prevail (Verizon, 2021). Unintentional threats include natural and other disasters, unplanned failures and errors in user data and systems. The American National Institute for Standards and Technology – NIST (Nieles et al., 2017) sorts vicious threats to information security in fraud and data theft; malware, hacker attacks, cyberespionage and insider threats; and unintentional in failures and errors at work, loss of equipment and documents and loss of privacy in sharing information publicly.

European Network and Information Safety Agency (ENISA, 2020a) sorts the most widespread contemporary cyberthreats in infection with various sorts of malware, web-based attacks, fraud or phishing, web application attacks, spreading of spam mails, denial of service, identity theft, insider threats, physical manipulation, damage, theft and loss as well as cyberespionage. Here, it is important to mention that social networks are increasingly used for attacks and data collection, and hacker attacks, attacks with social engineering and infections with malware, where *ransomware* represents a huge problem, are among the most problematic threats for organisations from the described (ENISA, 2020; Verizon, 2021).

Despite the prevailing external threats or external attacks on the information systems of organisations, a special challenge is represented by information threats coming from the insider environment, as it is harder to discover them in comparison with external threats (ENISA, 2018; Verizon, 2019). In case of the so-called *insider threat* that might be described as a situation when a person or a group connected to the victim (with access to the victim's information systems, networks and/or data) exceeds or abuses these access rights in a way that it has negative consequences for information security – i. e. creates risks for confidentiality, integrity or availability of information or information systems (ENISA, 2020b; CISA, n. d.). Insiders are persons with legitimate rights to access confidential or sensitive data and may be

- computer-related crimes (computer falsification and fraud),
- content-related crimes (children pornography),
- copyright crimes and crimes related to similar rights,
- racist and xenophobic actions and expressions of inappropriate statements towards genocide or crimes against humanity committed in computer systems (this group of actions is defined by the additional protocol to the Convention on cybercrime).

The convention prescribes that the signatory states take care for incrimination of the mentioned forms of crimes in their legal orders, take care of capability and capacity of immediate insurance of computer and traffic data, search of computer installations, interception of data and traffic as well as real-time insurance of data. The importance of international cooperation and support in investigations of cybercrime is stressed.

aware of the vulnerability of an information system (they may be employed, be ex-employees, contractors, business partners or collaborators) (Homoliak, Toffalini, Guarnizo, Elovici, & Ochoa, 2019; Jordan, Hawron, Jordan, & Hawron, 2015; S. L. Pfleeger & Stolfo, 2009; The CERT Insider Threat Center, 2016; Warkentin & Willison, 2009). The main reasons why violations and failures of employees or users appear may be comprised of five groups, as there are: lack of motivation to respect security rules; lack of knowledge of risks and attacks; inappropriate or risky convictions; inappropriate or risky behaviour; inappropriate use of technology (Badie & Lashkari, 2012). The worst abuses may happen mainly by privileged users, as they have knowledge of processes and systems in organisations, access to critical parts of a system and configurations of security mechanisms. Besides vicious (former or present) employees, who want to take revenge or damage an organisation for various reasons, a large problem is also unaware or careless employees or users, who enable an attack by external criminals by their negligence. Unaware and negligent users/employees may harm an organisation because of a disclosure of confidential information by error, reactions to phishing emails and malware, visits to inappropriate websites, thoughtless upload of contents, connecting equipment, enabling unauthorised access to data or information systems or because of losing or alienating electronic equipment and documentation (ENISA, 2017, 2018). Reports show that actually more than 80 % of all cyberattacks on organisations are connected to a human element, and among those where employees are the main cause, abuse of user rights and inappropriate handling of data prevail (Verizon, 2021).

Information vulnerability is defined as a security gap or weakness, error or deficiency in an information system (on the level of sources, processes or protection) (ISO/IEC 27000: 2018, 2018; Nieles et al., 2017) that alone does not cause negative consequences, yet. Negative consequences come up if vulnerability is used by information threats. Information vulnerability increases together with complexity and range of an information system. As information systems are composed of different elements, information vulnerability appears in different forms. Among the most targeted elements of information systems are servers, mobile equipment and laptops, as well as people or users (Verizon, 2021).

With the COVID-19 pandemic that caused drastic transformations in work processes and introduced home office or distant work in a majority of sectors, new challenges and risks connected to distant access, use of cloud technology, data transfer into private environments, sharing of files, video conference meetings and similar started to show up. During this time, criminals developed more personalised and sophisticated forms of user rights theft, phishing, social engineering, spreading of malware and attacks on mobile telephone platforms (ENISA, 2020). Among the main vulnerabilities connected to insider threats belongs e. g. inappropriate management of privileged rights, an increase of the amount of confidential data and an increase of the amount of equipment with access to confidential data, use of mobile equipment at the workspace, the high complexity of new technologies for users and the low degree of awareness among users (ENISA, 2017).

Besides the described elements, information security risks were finally strongly influenced by *security measures* (or security controls and mechanisms). Security measures are methods, rules or proceedings of organisations to oppose threats or correct vulnerabilities and to prevent or lower risks in this way.

In providing for information security situational surveillance measures (related to the use of mechanical, technical or software control) or managerial or organisational measures (activities related to addressing behavioural, procedural, political, environmental and normative aspects) may be taken. In line with this, international directives and normative acts, as a rule, divide information security measures into organisational (e. g., definition and formation of processes, accountability, education and training and raising of awareness), legal (e. g. providing for compliance, acceptance of policies, strategies, standing orders and agreements), logistical and technical (e. g. software control on the level of computers and user equipment, servers and databases, networks controlling and limiting access of traffic) and physical (e. g. physical obstacles, access control and protection from disasters) ones.

Measures of providing for information security may be divided into internal and external as well as preventive and reactive ones. External measures are mechanisms by which threats coming from the external environment of an organisation are mastered, and internal measures address threats coming from the internal environment. Preventive measures try to prevent the realisation of (situational or social) information incidents, while reactive measures are reaction mechanisms to

prepare an organisation for eventual incidents with the aim of an effective reaction, limitation of damage and healing (Allen & Westby, 2007; Kankanhalli, Teo, Tan, & Wei, 2003; Sethuraman & Adaikkappan, 2009). Measures may be more concretely divided further into measures of rejection (decrease of attractiveness or accessibility of a target), prevention (limitation and control of use of information systems); recognition (detection systems); and healing (normalisation of state after an incident) (Pfleeger & Pflegger, 2006).

The international expert organisation Center for Internet Security – CIS (2020) formed a list of 18 measures (*Critical Security Controls*) for cyberdefence that have been recognised as the most effective ways to stop contemporary threats and attacks. The list presented below represents a collection of high-priority measures formed in line with the *Parett* principle 80-20 that follows the idea that by executing a smaller collection of key activities, a major share of problems and vulnerability can be abandoned. The list, in line with international information security standards, has been developed since 2008 and is constantly updated regarding changes in technology development and threats. Measures are defined based on an analysis of the most frequent patterns of cyberattacks through sharing of knowledge and mutual adaptation and development by a vast consortium of governmental and industrial experts from different profiles.

1) Inventory or list of property and equipment of an organisation.
2) Inventory or list of software (definition of allowed and identification of unallowed software).
3) Data security (list and categorisation of data, security through the whole lifecycle).
4) Security configurations of the property and software of an organisation (e. g. possibility of remote control over equipment in case of theft or loss, configuration of firewalls, servers).
5) User account management (e. g., deletion of inactive, useless accounts, protection from hacker intrusion, attacks with raw force).
6) Access control management (e. g. multiple factor authentication, minimum privilege policy).
7) Continuous vulnerability management (e. g. regular updating of systems and implementation of security upgrades).
8) Surveillance of daily protocols.

9) E-mail and search engine security (e. g. antivirus protection, protection from unwanted e-mails, limitation of access to the homepage).
10) Protection from malware.
11) Data renewal capacity.
12) Network infrastructure management (e. g. updating and configuration of firewalls, routers, servers, administrator account safety).
13) Network supervision and safety (e. g. SOC, SIEM, IDS, IPS, VPN or centralised management, network segmentation, remote access security).
14) Raising awareness and training of users.
15) Management of connected subjects (partners, suppliers with emphasis on suppliers of cloud services).
16) Application security (e. g. security tests and application check-ups).
17) Incident reaction management (e. g. regular testing of plans).
18) Penetration tests.

In the phase of planning measures, it is important to have in mind that internal factors are those that most frequently enable the realisation of external threats. By focusing exclusively on technical aspects of security, an organisation might be protected from some external attacks and threats, but it still remains vulnerable to the most dangerous threats (Spears & Barki, 2010). Besides awareness programmes and user motivation, for the prevention of internal threats, an access and user rights management is of main importance. Only by preventive rules the possibility of abuse can be limited in a way that users obtain a range of use to the extent of obligatory necessity and exclusively to data connected to the content of their work (Bunker, 2012). From the point of view of surveillance, besides strong authentication processes in an organisation, so-called UBA (*User Behaviour Analytics*) solutions and procedures enabling surveillance of usage of a system and detection of anomalies or potential data abuse come to use more and more.

At individual scopes or groups of listed measures, various security solutions offered by different suppliers are at hand, but in the planning of measures, it is also necessary to have in mind rationality and functionality, as well as protection of the right to privacy. As already mentioned, namely, controls might be successful and provide for a high degree of security, but at the same time also irrational and ineffective (e. g. when too many measures are used or measures that are too limiting or invasive in relation to the level of risk). Hagen et al. (2008) say that information security

measures are effective when four pre-conditions are met: (a) when risks are at minimum level; (b) when investment in measures is rational and meaningful; (c) when measures are in line with provisions and legislation and (d) when users understand and really respect the measures.

4.3 Standards and Recommendations

When planning formation of ISMS and information security management, organisations dispose of support by different international standards. In Attachment A, some most well-reputed international standards and directives regulating field connected to information security management shall be comprised.
Following actual trends in the field of information security and cyberthreats, besides the mentioned standards, organisations may get support also by research and reports of various security enterprises and expert associations. Besides annual reports published by national response centres - CERT, among such reports published annually or periodically, are following:

- Cost of cybercrime study (Accenture and Ponemon).
- Data breach investigation report (Verizon).
- Global corporate IT security risk survey (Kaspersky).
- Global information security survey (Ernst & Young)
- Cybersurvey (Deloitte).
- Global state of information security survey (PWC).
- Cybersecurity breaches survey (Department for Digital, Culture, Media & Sport).
- Information security threat report (Symantec).
- Norton cybersafety insights report (Norton).
- Global cyber risk perception survey (Mesh and Microsoft).
- Threat landscape (ENISA).

5 Information Security and Higher Education Institutions

From the aspect of cyber and information threats, academic and research institutions belong among the most exposed organisations, as they manage numerous sensitive financial, academic and administrative data, mainly saved in electronic or digital form and by this, vulnerable to numerous attacks and abuses (Aguilar Quintero, Velásquez Pérez, & Castro Silva, 2019). In recent years, higher education institutions, with growing connectivity, face a huge increase in information security incidents, and therefore demands for a stronger personal data security and privacy are stepping into the foreground (EDUCAUSE, 2021; Ulven & Wangen, 2021). Since the needs for information security already exceed the capacities and accountability of individual technical staff or smaller departments in education institutions, a trend of frequent implementation of demands by international standards and establishment of specific workplaces like CISO and authorised personnel for personal data security can be seen in the past decade (Hommel et al., 2015).

Compared with other organisations, education institutions function under specific circumstances, strongly influencing needs in connection to information and cybersecurity. Vulnerability is high already due to the nature of the higher education branch that is based on academic freedom, openness, accessibility and transparency (including information systems and data), as well as due to the high level of digitalisation and connectivity (Campbell, n.d.; Hina & Dominic, 2017; Ulven & Wangen, 2021). Information systems and information technologies represent a critical and fundamental part of processes running in the higher education branch, and technological innovations represent the ground of its development and growth, while also vulnerabilities connected to data security and privacy of users increase (EDUCAUSE, 2021). From the aspect of processes, the culture of trust, connecting, cooperation and teamwork create an environment open for sharing and exchanging data (Adams & Blanford, 2003).

Among the special characteristics of education institutions, due to which they differ from other branches and that are important for information security, there also belong (Campbell, n.d.; Dell, 2018; EDUCAUSE, 2021; Fishman, Rudnicki, & Grama, 2021; Hommel et al., 2015; Ulven & Wangen, 2021; Vrhovec & Mihelič, 2021):

- Universities and departments manage enormous amounts of sensitive and confidential data (personal and financial data of employees, students, intellectual property, sensitive and confidential research data, data on partner organisations, etc.) because of what incidents in connection with abuse, theft of disclosure of these data lead to unimaginable consequences for the reputation of a university, as well as the safety of employees and students. Generally, a high degree of fluctuation of staff, students and visitors are characteristic for higher education institutions. Namely, on a daily level, there are many people or individuals who enter buildings and spaces of an institution as well as information systems.
- Interconnection of office and private life being traditional in an education and research institution is connected to the increasing use of private ICT for office purposes (*Bring Your Own Device* - BYOD). In education environments, the use of various portable or mobile equipment that connects to networks of the organisation is extraordinarily frequent, and in the same way, private and office data get joined on users' or staff's equipment. Mobile equipment represents an extra high vulnerability or risk, as students, visitors, as well as employees connect with their various mobile and smart equipment to networks, access data and applications.
- Servers managed by higher education institutions and accessible via the internet represent an attractive target to criminals. Namely, besides data, infrastructural sources, such as high-performance processors, networks and servers are interesting to them, as by the manipulation of these, sophisticated DDoS attacks can be performed, or malware or spam can be distributed.
- Increasing distance education increases the use of open internet learning environments, videoconferencing tools and data sharing via the internet. Today, pedagogical processes and students prevailingly work in a digital environment, many processes and functions are conducted through the internet. Even connections between different education institutions and researchers are increasingly intensive and frequent, which results in an implementation and use of complex tools and environments for collaboration. In times of pandemic, vulnerabilities in connection to the use of new technologies have increased, since there was a total move of pedagogical and research activities into cyberspace.

- Vulnerabilities are also represented by advanced technologies that are being introduced to support innovative forms of education and training, as there are virtual and augmented reality (VR and AR). The use of such technologies is frequent for the needs of simulation (e.g., in fields of natural sciences and technologies) and realistic collaborations. These systems frequently are weakly protected and vulnerable to intrusion and abuse (e.g., do not use coded network connections; users use personal equipment bypassing established protocols for authentication; offenders create a twin profile or avatar or use vulnerability of sensors, cameras and microphones). Attackers may abuse mentioned vulnerabilities to gain access to tools and applications for cooperation and destruction, data, communication or infection of an organisation's network.
- For the education branch, fragmentation of networks and mutual connectivity of these networks is characteristic, as well as a vast inter-organisational environment creating a wide network of connected systems and data. Further, the use of services and data saving in clouds becomes more frequent, creating new or larger vulnerabilities and possibilities of abuse.

To sum up, higher education institutions have a great challenge represented by their need to a parallel balancing of demands for security, resilience, and surveillance on the one side and needs for openness, accessibility connectivity, privacy, innovation and flexibility on the other side.

5.1 Information Security Risks in Higher Education

One of the most important information properties managed by education and research institutions that can be subject to abuse are data on students, financial data, research data and data on employees. In addition to these data that belong to the most sensitive data, also other data are relevant for information security, e. g., study materials, learning plans, exams, and leadership and management data (Ulven & Wangen, 2021). Mainly research cognitions and achievements belong to the most targeted data and information (EDUCAUSE, 2021; ENISA, 2020), as well as personal data and user names and passwords (Verizon, 2021).

Among the most frequent cyberthreats endangering the education branch, ENISA (2020) ranks malware, ransomware, internet attacks, and in the past year, even an increase of cyberespionage was noted. As a consequence of a vast amount of data managed by education institutions, in such a branch, one can notice a trend of increased targeted attacks (Hommel et al., 2015). For higher education institutions, attacks with social engineering are a huge problem since more than a third of data abuse is connected to such a threat (Impact, 2021). A study on susceptibility and vulnerability by phishing attacks between different branches and industries showed that the education branch ranks in fourth place (thus among the most vulnerable branches), with a success rate of phishing fraud of 13 % (Proofpoint, 2021). In its annual report, also Verizon (2021) lists social engineering attacks among relevant threats to higher education institutions in the same way also (D)DoS attacks that represented more than half of the attacks on the education branch in 2019. From the aspect of malware, ransomware represents the largest threat and the majority of infections in higher education institutions. In addition to the mentioned, a frequent cause of incidents are also attacks by employees e. g., by intentional disclosure of data or wrong use of systems as well as violations of policies, loss or theft of electronic equipment (Ulven & Wangen, 2021).

Among criminals targeting the education branch, financially motivated and highly capable hackers prevail. With sophisticated techniques and methods, they aim at obtaining and selling personal or confidential data or want to use capacities or capabilities of the technologies managed by higher education institutions in order to conduct other attacks. Besides financially motivated hackers, activists and those, who act for the purpose of state-supported espionage, represent a frequent group of criminals, as well. Incidents are also connected to the criminals, who want to cause intentional damage or breakdown of information systems or test security protocols, not rarely also disappointed students or (ex) employees, who want to take revenge, appear among the criminals (Dell, 2018; Ulven & Wangen, 2021; Verizon, 2021).

A study from 2020 among 500 employees from higher education branches showed that more than a third of education institutions had witnessed a caber attack in the past, and one-fifth had witnessed such an attack during the time of pandemic (Morphisec, 2020). A study conducted among higher education institutions in Great Britain showed very similar results since in the period from 2015 to 2020, 33 % of the education institutions went through an attack with ransomware (TopLine

Comms, 2020). In the past two years (2019-2021) or during the time of the global COVID-19 pandemic, respectively, in higher education institutions, numerous critical and medical exposed information security incidents were realised. Below, some most well-known are exposed:

- Australian National University: a hacker attack caused data abuse of 200.000 people.
- University of Greenwich: compromising of sensitive data of 19.500 students resulted in a fine of 160.000 dollars.
- Washington State University: an infection with malware led to abuse of personal data of 4.5 million people.
- University of Connecticut: a hacker attack led to compromising of personal data of 326.000 people.
- Monroe College: an infection with ransomware led to a payment of 2 million dollars in ransom.
- University of California: an infection with ransomware led to a payment of 1.14 million dollars in ransom.
- German University Hospital Düsseldorf: an infection with ransomware resulted in a victim of death.
- Harrison Federation: an infection with ransomware disabled 37.000 pupils of elementary schools in Great Britain from accessing e-mail.

Besides the mentioned, other universities were victims of ransomware, as well (e. g., Oregon State University, Michigan State University, Kent State University, University of Dayton, Columbia College University, and in the USA, even several elementary and secondary schools (*K-12 Schools*) were victims of such attacks (Morphisec, 2020).

Vulnerabilities appearing in the higher education branch and representing an opportunity for criminals and increase risks are of organisational as well as of technological nature. From the technical point of view, in higher education institutions inadequate e-mail security frequently represents a problem, as well as processes of user rights management (Verizon, 2021). Undeveloped or weakly developed detection and reaction capacities, inadequate authentication processes and information system access management also represent an important challenge

(EDUCAUSE, 2021). Because of the culture of openness, frequently also strong physical controls connected to entry and exit an absent or rare (FireEye, 2014). Ulven & Wangen (2021) list inadequate management of mobile equipment; inadequate data protection protocols through processes of data obtaining, creation, saving, processing and transfer; absence of technical key measures defined as good practice and vulnerabilities connected to complexity and splitting of networks among the main technical vulnerabilities of higher education institutions.

Employees belong to important vulnerabilities of education institutions, as well, as almost half of the incidents are connected to employees and their failures at work (Verizon, 2021). From this aspect, mainly a lack of awareness and training management for staff and students is representing a problem and in addition to that also an inadequately developed security management and information security management approach, a lack of leadership support and an improper attitude towards information security as such (Ulven & Wangen, 2021). According to this, mainly a lack of a holistic approach to system security management that is supposed to upgrade technical measures and to include activities directed to the development of a strong security culture among employees and students is stressed to be an important challenge (Hina & Dominic, 2017).

It also must be mentioned that higher education institutions were among the first branches that followed the trends of digitalisation, and this is why the first-aged systems are still in use and they are highly vulnerable. Due to decentralisation, autonomy and high variability among individual departments or institutes, ICT management and security is also frequently decentralised, which hinders transparency, unified management and quick response. Like in other branches, higher education faces a lack of specialised personnel in the field of information an cybersecurity. (Campbell, n.d.; EDUCAUSE, 2019b, 2021; FireEye, 2014). In 2018, more than half of higher education institutions (n = 3,800) still did not possess regularly employed staff for the field of information security. Also, a lack of financial resources represents a problem and disables the use of contemporary security solutions. Namely, higher education institutions prevailingly are publicly financed and cannot afford higher financial investments enabling the purchase of more updated solutions. An overview of state-of-the-art from 2018 also showed that higher education institutions dedicated only 3,6% of the total IT budget for IT security (EDUCAUSE, 2019b). Consequently, higher education institutions

frequently are capable only of reactive functioning (response to incidents), but proactive security from more contemporary threats is not developed (Dell, 2018; Fishman et al., 2021).

For providing for an adequate level of information security and in this context for privacy and personal data security, as well, the most important measures that should be taken by higher education institutions are (Buzzelli, 2021; Campbell, n.d.; Ulven & Wangen, 2021):

- access control mechanisms, which include a multi-layer authentication, a minimum privilege policy as well as physical security of location and equipment from abuses, damages, theft, accidents, etc.
- identification and prioritisation of critical systems and data management throughout the whole lifecycle (protocols connected to digitalisation, transfer, sharing of data, archiving, destruction, access or collection).
- maintenance of audit trails, and verification of integrity.
- safety copies, regular updates and security reparations.
- internet attack security, mainly security from SQL and phishing attacks, e-mail security management, data and communication traffic surveillance, and network segmentation.
- development of holistic information security management including a centralised approach to policy management and adoption (e. g. data security, constant functioning, responses to incidents, and management).
- development of an accountability and awareness culture among employees and students, which includes a strong management system and awareness campaign.

Cheung (2014) defines similar measures mentioning that information security management in higher education institutions should include measures conducted or implemented in eight fields:

- data security,
- security culture and accountability of employees,
- physical security,
- access control,

- communication and commercial process safety,
- information system safety,
- incident management,
- continuous functioning management.

Based on an extensive overview of the literature on the topic of information security incidents and risks in the education branch, Ulven & Wangen (2021) proposed or developed a model of information security elements in higher education institutions. Based on their findings, we created a graphic demonstration of such elements and their connections, shown in table 2.

Table 2: Model of information security elements and information security risks in higher education institutions*

Elements \ Incidents		Intruding, infection	Vulnerab. scans	Targeted attacks	fails	Data, equip. theft/loss	kidnapping	Abuse of infrastructure	Internal threats	DDos Attacks
Vulnerabilities	Technical controls	x	x	x				x	x	x
	Data control				x					
	Physical controls					x				
	Mobile equip.	x								
	Passwords	x					x			
	Management				x	x		x		x
	Awareness	x		x	x		x			
	Security culture	x		x	x			x	x	
	Resources		x							x
	Complexity	x	x							x
Motives	Financial	x	x	x		x	x			x
	Espionage	x	x	x			x			
	Grief, revenge							x	x	
	Activism									x
	Opportunism		x			x		x		x
	Unintended fails				x	x		x		x
Sources	Digital data	x		x	x		x		x	
	ICT infrastructure	x	x					x	x	x
	Personal equip.					x				
	Physical data					x				
Consequences	Data loss	x				x	x		x	
	Data flow	x		x	x		x		x	
	Loss of access	x	x		x			x	x	x
	Data abuse		x				x	x		
	Fraud			x						
	Loss of integrity				x				x	
	Loss of equip.					x				

* The table was made based on data obtained from Ulven & Wangen (2021) including an analysis of 2984 information events noted in higher education between 2017 and 2019 in 10 different sources of literature.

6 Conclusion

Modern times are marked by digitalisation and cybercrime. A pro-active approach to providing information security is of key importance not only for survival but also for the public reputation and competitiveness of an organisation.

Challenges and risks in the field of information security are practically faced by all industries and organisations, disregarding the nature of the branch. There, the higher education branch is no exception, quite the opposite; because of its specific nature (culture of openness, accessibility, and connections), a high amount of confidential data, a high fluctuation of people and a high level of digitalisation and inclusion in cyberspace information security risks are especially high and strongly endanger personal data security, privacy and by this the public reputation of institutions. An overview of the state-of-the-art in the higher education and education branch shows that a lack of adequate technical controls, an underdeveloped security management, a weak awareness of employees and students and a generally low-security culture belong to the main vulnerabilities. Hacker attacks, malware (especially ransomware), DDoS attacks, social engineering attacks (especially phishing attacks), theft and loss of electronic equipment and abuse of user accounts and data most frequently cause incidents. Among the most frequent consequences of incidents, there is a loss, flow or abuse of data and loss of access to them. Among the criminals, financial motives, espionage. Opportunism and also fails of employees prevail. Intentional threats most frequently aim at research and personal data, but also the highly capable infrastructure. In the future, from the aspect of measures, technical security with the implementation of more advanced detection and surveillance mechanisms and from the aspect of management providing for a holistic approach including fostering of awareness and a culture of responsibility on the level of leadership and employees as well as on the level of students must be upgraded.

In a system of providing for information security, it is most important to become aware that social elements are the ones, on which it depends most, whether an organisation will be capable of fighting contemporary threats and defending from cyberattacks. It is a matter of fact that technical measures and control cannot prevent all threats, especially not those connected to the behaviour of users or the use of information systems. Thus, it is for the employees in an organisation to contribute to strong information security or to represent its main vulnerability.

When employees are aware of the rules and threats when they respect policies and act responsibly, they can prevent the realisation of many external threats, but in the opposite case by irresponsible acting and risky behaviour, they make it easy for external threats or enable execution of an attack and by this contribute to the realisation of incidents (Kearney, 2010). People's behaviour is a more unreliable and unpredictable component of information security than technical solutions. Therefore the social sub-system is also much harder to be managed than the technical one. It is therefore not surprising that experts are generally convinced that employees are the weakest part in the information security chain, while higher education institutions are no exception, of course (Hina & Dominic, 2017; Metalidou et al., 2014). From this aspect, it is important that organisations have a holistic management system that also includes organisational and socially oriented activities and measures. In the first place, it is important that a clear vision and a system of rules and accountability is set up and that this is formalised in an information security strategy and policy. Namely, a policy is the backbone of management and the ground of a good information security plan. A system of rules may encompass several kinds of policies, instructions and standing orders, where accountability, demands, processes and control and disciplinary measures are defined. For a successful implementation of policies in practice, it is essential that users get acquainted with it, that they understand the demands and pre-conditions or that it clearly derives from its contents what are their responsibilities and liabilities in the use of information systems and data. But, as Metalidou et al. (2014) stress, the rationality of rules and demands that must have a minimum influence on the productivity and labour of employees must not be neglected because, in the opposite case, employees will find ways of circumvention.

Thus, it is of key importance that rules are clear, unambiguous and understandable. In the same way, it is important that users or employees are trained for execution and motivated for respect. Each employee or user in an organisation should be aware of what responsibilities have been delegated to him or her, how to behave and how to respond in case of facing potential threats (K. Thomson & Niekerk, 2012). In processes of training and awareness building, not only questions on what to do and how to behave must be answered, but also why. Understanding the danger of consequences of information security risks for an organisation can motivate employees to higher compliance (Kearney, 2010). Orshesky (2003) says that the best and easiest way to reach simple, understandable and executable rules and policies for

employees is to include employees already in the development and later implementation of policies at the highest possible level. People, who are part of the process of forming rules, feel more obliged and responsible to follow them and, at the same time, invite others to respect them than when policies are merely dictated or forced upon them.

If organisations wish to reach compliance of user and employees' behaviour with prescribed demands, processes of raising awareness[3] and training, as well as fostering legitimacy[4] of information security among users are inevitable. Since in an organisational environment one must not neglect influence of social learning and group dynamics on people's behaviour, it is of the same importance to develop a positive security culture[5].

Literature

Adams, A., & Blanford, A. (2003). Security and Online Learning. In C. Ghaoui (Ed.), Usability Evaluation of Online Learning Programs (pp. 331–359). https://doi.org/10.4018/978-1-59140-105-6.ch018

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy006

Aguilar Quintero, N. A., Velásquez Pérez, T., & Castro Silva, H. F. (2019). Information security model. Case study higher education institution. Journal of Physics: Conference Series, 1257(1). https://doi.org/10.1088/1742-6596/1257/1/012014

Allen, J. H., & Westby, J. R. (2007). Governing for enterprise security: Implementation guide. Article 1 - Characteristics of effective security governance. Pittsburgh: Carnegie Mellon University.

Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 367(1898), 2717–2727. https://doi.org/10.1098/rsta.2009.0027

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. Journal of Basic and Applied Scientific Research, 2(9), 9331–9347.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Information & Management Incident-centered information security : Managing a strategic balance between prevention and response. Information & Management, 51(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Bernik, I. (2014). Cybercrime: The costs of investments into protection. Varstvoslovje, 16(2), 105–116.

[3] Information security awareness refers to a level of awareness by users on the relevance of information security and knowledge of rules regarding information source security (Khan, Alghathbar, Nabi, & Khurram, 2011).

[4] Information security is legitimate, when employees understand it as reasonable, needed and wishful and just, and measures are functional and have a minimum influence on the workflow (Son, 2011).

[5] Information security culture can be defined as value, opinion and behaviour system developed among employees in the use of information, information systems and cyberspace and influencing information security (Da Veiga & Eloff, 2010).

Bernik, Igor, & Prislan, K. (2016). Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. PLOS ONE, 11(9). https://doi.org/10.1371/journal.pone.0163050

Boersma, J., Loke, G., Petkova, V. T., Sander, P. C., & Brombacher, A. C. (2004). Quality of information flow in the backend of a product development process: A case study. Quality and Reliability Engineering International, 20(4), 255–263. https://doi.org/10.1002/qre.551

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. International Journal of Information Management, 28(5), 413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

BSI. (2018). ISO 27001 Information Security Features and Benefits. Retrieved from https://www.bsigroup.com/LocalFiles/en-SG/ISO 27001 SG/ISOIEC 27001-Features-and-Benefits (SG).pdf

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. Information Security Technical Report, 17(1–2), 19–25. https://doi.org/10.1016/j.istr.2011.12.002

Buzzelli, M. E. (2021). Protecting and Ensuring Student Privacy. Retrieved from Inside Higher Ed website: https://www.insidehighered.com/views/2021/04/16/key-steps-take-protect-student-records-and-ensure-cybersecurity-opinion

Campbell, S. (n.d.). Cybersecurity in Higher Education: Problems and Solutions. Retrieved from Toptal website: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

Center for Internet Security. (2021). CIS Controls. Retrieved from https://learn.cisecurity.org/cis-controls-download

Chang, E. S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345–361. https://doi.org/10.1108/02635570610653498

Cheung, S. K. S. (2014). Information security management for higher education institutions. Advances in Intelligent Systems and Computing, 297, 11–19. https://doi.org/10.1007/978-3-319-07776-5_2

Convention on Cybercrime. (2001). Retrieved from https://rm.coe.int/1680081561

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers and Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

de Oliveira Albuquerque, R., Villalba, L., Orozco, A., Buiati, F., & Kim, T.-H. (2014). A Layered Trust Information Security Architecture. Sensors, 14(12), 22754–22772. https://doi.org/10.3390/s141222754

Dell. (2018). Higher Education Security Whitepaper. Retrieved from https://www.delltechnologies.com/asset/en-ca/solutions/industry-solutions/industry-market/dell_hi_ed_security_whitepaper.pdf

EDUCAUSE. (2019a). Information Security Guide: Effective Practices and Solutions for Higher Education. Retrieved from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide

EDUCAUSE. (2019b). The EDUCAUSE Information Security Almanac. Retrieved from https://library.educause.edu/resources/2019/4/the-educause-information-security-almanac-2019

EDUCAUSE. (2021). 2021 EDUCAUSE Horizon Report: Information Security Edition. Retrieved from https://library.educause.edu/-/media/files/library/2021/2/2021_horizon_report_infosec.pdf?la=en&hash=6F5254070245E2F4234C3FDE6AA1AA00ED7960FB

ENISA. (2015). ENISA Threat landscape: Overview of current and emerging cyber-threats. Retrieved from https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

ENISA. (2017). Baseline security recommendations for IoT in the context of critical information infrastructures. Retrieved from https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

ENISA. (2018). ENISA Threat landscape report 2017. 15 Top cyber-threats and trends. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport

ENISA. (2020). ENISA Threat Landscape 2020. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

EU Security Union Strategy. (2020). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

European Crime Prevention Network. (2016). Cybercrime: A theoretical overview of the growing digital threat. Retrieved from https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf

Eurostat. (2020). ICT usage in enterprises in 2019. Retrieved from https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

Ezingeard, J. N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. Information Systems Management, 22(2), 20–29. https://doi.org/10.1201/1078/45099.22.2.20050301/87274.3

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences, 256, 57–73. https://doi.org/10.1016/j.ins.2013.02.036

FireEye. (2014). Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do About It. Retrieved from https://www.fireeye.com/current-threats/threat-intelligence-reports/wp-storming-the-ivory-tower.html

Fishman, T., Rudnicki, R., & Grama, J. L. (2021). NIST Special Publication 800-171 for higher education A guide to helping colleges and universities comply with new federal regulation. Retrieved from Deloitte Insights website: https://www2.deloitte.com/us/en/insights/industry/public-sector/protecting-classified-uncontrolled-information-higher-education.html

Furnell, S., & Moore, L. (2014). Security literacy: The missing link in today's online society? Computer Fraud and Security, 2014(5), 12–18. https://doi.org/10.1016/S1361-3723(14)70491-9

Goodyear, M., Portillo, S., Goerdel, H. T., & Williams, L. (2010). Security officers: Strengthening cybersecurity series. Washington: IBM Center for The Business of Government.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management and Computer Security, 16(4), 377–397. https://doi.org/10.1108/09685220810908796

Hina, S., & Dominic, D. D. (2017). Need for information security policies compliance: A perspective in Higher Education Institutions. International Conference on Research and Innovation in Information Systems, ICRIIS, 1–6. https://doi.org/10.1109/ICRIIS.2017.8002439

Hommel, W., Metzger, S., & Steinke, M. (2015). Information Security Risk Management in Higher Education Institutions : From Processes to Operationalization. EUNIS Journal of Higher Education IT, (2015/3), 1–12.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys, 52(2). https://doi.org/10.1145/3303771

Impact. (2021). 15 Cybersecurity in Education Stats You Should Know for 2020. Retrieved from https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/

Interpol. (2021). Cybercrime: Cyberattacks know no borders and evolve at a rapid pace. Retrieved from https://www.interpol.int/Crimes/Cybercrime

ISO/IEC 27000:2018. (2018). Information technology - Security techniques - Information security management systems - Overview and vocabulary. Geneva: International Organization for Standardization, International Electrotechnical Commission [ISO/IEC].

ISO/IEC 27005:2018. (2018). Information technology - Security techniques - Information security risk management. Geneva: International Organization for Standardization, International Electrotechnical Commission [ISO/IEC].

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Kearney, P. (2010). Security: The Human Factor. Cambridgeshire: IT Governance Pub.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khurram, M. (2011). Effectiveness of information security awareness method based on psychological theories. African Journal of Business Management, 26(5), 10862–10868.

Klimoski, R. (2016). Critical Success Factors for Cybersecurity Leaders: Not Just Technical Competence. Retrieved from People + Strategy Journal website: https://www.shrm.org/executive/resources/people-strategy-journal/Winter2016/Pages/success-cybersecurity.aspx

Laţici, T. (2019). Cyber: How big is the threat? Retrieved from http://www.europarl.europa.eu/thinktank

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of it business value. MIS Quarterly: Management Information Systems, Vol. 28, pp. 283–322. https://doi.org/10.2307/25148636

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., & Skourlas, C. (2014). Human factor and information security in higher education. Journal of Systems and Information Technology, 16(3), 210–221. https://doi.org/10.1108/JSIT-01-2014-0007

Mishra, S., & Chasalow, L. (2011). Information Security Effectiveness: A Research Framework. Issues in Information Systems, XII(1), 246–255. https://doi.org/10.48009/1_iis_2011_246-255

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from Cybercrime Magazine: Special Report: Cyberwarfare In The C-Suite website: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Morphisec. (2020). Education Cybersecurity Threat Index. Retrieved from https://engage.morphisec.com/education-cybersecurity-threat-index

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision : An Introduction to Information Security. https://doi.org/10.6028/NIST.SP.800-12r1

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. International Journal of Information Management, 49(April), 208–216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

Orshesky, C. M. (2003). Beyond technology – The human factor in business systems. Journal of Business Strategy, 24(4), 43–47. https://doi.org/10.1108/02756660310494872

Osborne, M. (2006). How to cheat at managing information security. Rockland: Syngress Publishing.

Pesante, L. (2008). Introduction on information security. Pittsburgh: Carnegie Mellon University.

Pfleeger, C. P., & Pflegger, S. L. (2006). Security in computing (4th ed.). Upper Saddle River: Prentice Hall.

Pfleeger, S. L., & Stolfo, S. J. (2009). Addressing the insider threat. IEEE Security and Privacy, 7(6), 10–13. https://doi.org/10.1109/MSP.2009.146

Prislan, K., & Bernik, I. (2019). Informacijska varnost v organizacijah. Maribor: Univerzitetna založba Univerze v Mariboru.

Prislan, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. PLOS ONE, 15(9). https://doi.org/10.1371/journal.pone.0238739

Proofpoint. (2021). Threat report: State of the Phish Report. Retrieved from https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. Information Systems Frontiers, 19(5), 1205–1228. https://doi.org/10.1007/s10796-016-9648-8

Seese, M. (2009). Scrappy information security: The easy way to keep the cyberwolves at bay. Silicon Valley: Scrapy About.

Sethuraman, S., & Adaikkappan, A. (2009). Information security program: Establishing it the right way for continued success. ISACA Journal, 5, 1–7.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information and Management, 48(7), 296–302. https://doi.org/10.1016/j.im.2011.07.002

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly: Management Information Systems, 34(Spec. Issue 3), 503–522. https://doi.org/10.2307/25750689

Tayaksi, C., Ada, E., Kazancoglu, Y., & Sagnak, M. (2021). The financial impacts of information systems security breaches on publicly traded companies: reactions of different sectors. Journal of Enterprise Information Management. https://doi.org/10.1108/JEIM-11-2020-0450

The CERT Insider Threat Center. (2016). Common Sense Guide to Mitigating Insider Threats, Fifth Edition. Retrieved from https://www.odni.gov/files/NCSC/documents/nittf/20180209-CERT-Common-Sense-Guide-Fifth-Edition.pdf

The EU's Cybersecurity Strategy for the Digital Decade. (2020). Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

Thomson, K. L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. Computer Fraud and Security, 2006(5), 11–15. https://doi.org/10.1016/S1361-3723(06)70356-6

Thomson, K., & Niekerk, J. Van. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. Information Management and Computer Security, 20(1), 39–46. https://doi.org/10.1108/09685221211219191

TopLine Comms. (2020). UK university ransomware FoI results. Retrieved from https://toplinecomms.com/insights/uk-university-ransomware-foi-results

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), 1–40. https://doi.org/https://doi.org/10.3390/fi13020039

Verizon. (2019). Insider Threat Report. Retrieved from https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

Verizon. (2021). Data breach investigation report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

von Solms, B. (2001). Information security - A multidimensional discipline. Computers and Security, Vol. 20, pp. 504–508. https://doi.org/10.1016/S0167-4048(01)00608-3

von Solms, B. (2010). The 5 Waves of Information Security-From Kristian Beckman to the Present. In K. Rannenberg, V. Varadharajan, & C. Weber (Eds.), Security and Privacy – Silver Linings in the Cloud. SEC 2010. IFIP Advances in Information and Communication Technology, vol 330. (pp. 1–8). https://doi.org/https://doi.org/10.1007/978-3-642-15257-3_1

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. Computers and Security, 106. https://doi.org/10.1016/j.cose.2021.102309

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101–105. https://doi.org/10.1057/ejis.2009.12

Whitman, M. E., & Mattord, H. J. (2012). Principles of information security (4th ed.). Boston: Course Technology, Cengage Learning.

Annex A: Standards and Guidelines

ISO/IEC 27000 (*Information technology – Security techniques – Information security management systems – Overview and vocabulary*). Description: textual, glossary giving a general overview of the information security management system and explanations on expert terminology and definitions usually utilised in the ISO 27000 standards series.

ISO/IEC 27001 (*Information technology – Security techniques – Information security management systems – Requirements*). Description: the standard represents demands for formation, execution, maintenance and permanent improvement of the information security management system in organisations - ISMS. ISMS is a general management framework enabling an organisation to identify, analyse and handle information security risks. In case of a certification, organisations must determine how specific fields and controls defined in the standard are dealt with.

ISO/IEC 27002 (*Information technology – Security techniques – Code of practice for information security controls*). Description: the standard contains instructions widening and thoroughly describing information security management control defined in the standard ISO/IEC 27001. It is a code of conduct used by organisations as guidelines for obtaining the ISO/IEC 27001 certificate.

ISO/IEC 27003 (*Information technology – Security techniques – Information security management systems – Guidance*). Description: the standard includes directives for information security managers on approaches and ways of planning and execution of implementation of the ISMS system and recommendations after ISO/IEC 27001.

ISO/IEC 27004 (*Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*). Description: Gives directives for assessment of success and effectiveness of the information security management system (processes, surveillance and control).

ISO/IEC 27005 (*Information technology – Security techniques – Information security risk management*). Description: the standard gives directives for mastering information security risks and supports general concepts determined in ISO/IEC 27001. The standard gives starting points to be followed by an organisation in formation of its risk management system.

ISO/IEC 27031 (*Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*). Description: the standard describes how to provide for readiness for constant operation on ICT level. It is about an upgrade of the incident management system.

ISO/IEC 27032 (*Information technology – Security techniques – Guidelines for cybersecurity*). Description: the standard gives directives for providing for and development of cybersecurity in organisation in fields, as there are: information security, network and internet security, critical and key infrastructure security.

ISO/IEC 27035-1 and **ISO/IEC 27035-2** (*Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management / Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*). Description: a standard for incident management composed of two parts. The first part of the standard defines basic concepts and defines key phases of reaction to incidents (detection, reporting, assessment, response). The second part contains directives and instructions for formation of a plan and preparation of s response, together with good practices.

ISO 22301 (*Security and resilience – Business continuity management systems – Requirements*). Description: a standard for constant activity performance, listing pre-conditions for planning, execution, management, surveillance and maintenance of a system in an organisation for protection from interruption of activity. It describes how to respond to events and how to tackle renewal of activity and gives directives for risk reduction, as well. Demands are general and meant for use in all organisations. The range of these demands depends on the environment and complexity of an organisation.

ISO/IEC 15408-1 (*Information technology – Security techniques – Evaluation criteria for IT security*). Description: the standard determines security matters and common criteria for assessment or testing of information security technology. It describes criteria to be met by computer products tested and certified for security aspects.

Standard of Good Practice (publisher: Information Security Forum - ISF). Description: Standard of Good Practice is meant for leaders and managers of information security, IT managers, internal and external auditors and IT suppliers as a practical handbook for the detection and management of risks in the field of information security in organisations and their supply chains.

Cybersecurity Framework (publisher: NIST). Description: a framework for providing for cybersecurity, giving directives to organisations in the formation of cybersecurity and cyber risk mastering based on existing standards, instructions and good practice. The framework is mainly meant for systems of critical infrastructure. It gives a taxonomy of wishful organisational states and results and describes the realisation of these goals with respect to normative demands regarding the protection of privacy and personal data.

Special Publications 800 series (publisher: NIST). Description: a series of more than 190 standards or publications handling most various aspects of providing for information and cybersecurity (from general concepts to technical solutions), or giving directives for specific branches.

IASME (*Information Assurance for Small to Medium-sized Enterprises Governance Standard*). Description: the standard describes criteria for data security in smaller enterprises.

COBIT 5 for Information Security (publisher: ISACA, *Control Objectives for Information and Related Technology - COBIT: A business framework for the governance and management of enterprise IT*). Description: commercial framework for leading and managing information security technologies in organisations. It gives concrete instructions regarding formation of a proper organisational structure and culture being the base for a high level of information security. It includes a methodology for assessment and evaluation of information security maturity.

PAS 555 (publisher: British Standard Institution – BSI, *Cyber security risk. Governance and management. Specification*). Description: a general business model for information security management in organisations and a complete partner chain. It contains as technical as well as user and organisational aspects. It is the result of an initiative by larger IT enterprises. It describes roof pre-conditions and fields to be regulated for providing for a holistic approach to security and an according interconnection between the fields.

BS 10012 (publisher: British Standard Institution – BSI, *Personal Information Management System*). Description: recommendations for providing for privacy and personal data security in line with demands by General Data Protection Regulation (GDPR).

BS 7799 (publisher: British Standard Institution – BSI, *Information Security Risk management*). Description: the standard describes processes and procedures relevant for information security risk management in organisations. Directives are compliant with ISO/IEC 27001 and general Data Protection Regulation (GDPR).

BSI-Standard 100-3 (publisher: Bundesamt für Sicherheit in der Informationstechnik – BSI, *Risk analysis based on IT-Grundschutz*). Description: the standard presents a methodology and a process for risk assessment in the field of data processing in line with the classification of threats and risks defined in the IT-Grundschutz catalogue (Germ. GSK).