Risk as the Cornerstone of Information Security and Data Protection

COLIN, Jean-Noel

Published in:
Deep diving into data protection

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Risk as the Cornerstone of Information Security and Data Protection

Jean-Noël Colin[1]

Introduction

Over the last decades, our society as a whole has witnessed an explosion of services qualified as 'e-' or 'smart-'. Almost no human activity escapes this interference, sometimes impacting our existences in a very intrusive way: e-health, e-government, e-banking, e-learning, smart cities, smart home, smart farming, smart grid… all dematerialize and create an abstract digital replica of our lives, to which we accept an always increasing dependency. This raises questions, when the services become unavailable or do not perform reliably. Moreover, creating, maintaining, and exploiting those replicas most of the time require the sharing of – often – sensitive data, between information systems owned and run by bodies for which is it hard, not to say impossible, to determine the level of security they give to our information.

Information Systems (IS) are highly complex constructions, whether at the level of functionalities they offer or regarding the technological architectures on which they rely, hardware and software. This induces a real risk of loss of understanding and control of the system, threatening the security of the data stored and processed, as well as of the services themselves. In addition, those complex architectures involve multiple stakeholders, sometimes operating in distant locations, between which trust is relative and often limited to digital exchanges. This can be problematic, for instance when it comes to settling responsibilities in case of conflict.

Paradoxically, the user of such system, albeit often without a true alternative being available, has little to no means to evaluate the security of the systems that hold and process his data. On the one hand, such evaluation would require specialized skills usually not present with the ordinary citizen, but on the other hand, lack of information from the system owners also makes the task impractical.

[1] University of Namur, Faculty of Computer Science, CRIDS/NaDI.

To efficiently analyze the security of an IS, it is critical to model and describe it in a precise way, identifying its components with their functions and their location, the stakeholders with their roles and responsibilities. It is then mandatory to define its security requirements and evaluate them on a scale, in order to elaborate a security plan as a list of measures or controls that allow the system to meet those requirements. Without a proper and accurate evaluation, there is a risk to under-protect or over-protect the IS, with negative consequences in both cases. One must admit though that often, security is the poor relation of the IS, and is neglected in front of other business or organizational imperatives.

Among other things, data protection implies and requires that "appropriate technical and organizational measures to ensure a level of security appropriate to the risk[2]" be implemented. It is thus a regulatory requirement to guarantee proper protection to data. The same regulation also gives rights to the data subject, like right to access, rectification, erasure or portability… This can have a huge impact on the design of an Information System which needs to be built in such a way that it is practically possible to respond to an individual seeking the exercise of one of those rights.

Data protection is an important driver for information security. However, other reasons exist that force any organization to take security seriously and adopt a structured, measurable approach to manage it. A widely adopted approach for securing an IS is based on the concept of risk, which allows to identify, measure, prioritize the elements of the information system to protect and define the measures to be put in place for its protection. We strongly advocate for such an approach, which can be tailored to meet various kinds of situations and help in many contexts to continuously improve the level of security given to data.

In this chapter, we summarize how information security, which encompasses data protection, can be perceived and formalized at a technical level. We start by proposing a structured view of an Information System and its security requirements. We also advocate the need for any actor of the society, company, administration or individual, to adopt a security posture in line with its own objectives and requirements, and we describe the consequences he might face in case proper protection is not implemented. Next, we present a common approach for analyzing and improving the security of an IS, namely a risk management process, based on ISO 27000 family of standards. In the last section, we gather general security principles that should govern any security plan and describe a set of generic security measures.

[2] General Data Protection Regulation 2016/679, art. 32.

1. Information System Security

1.1. Defining the Information System

In general, a computer system can be described as an electronic system able to store, process and exchange data. This definition equally applies to a personal computer, a mainframe, a tablet, a robot, or a smart thermostat.

An Information System is a higher-level concept, that integrates technological components like computer systems as defined above, but also organizational elements and human actors that take part in the construction, operation, maintenance of the IS, or simply use it as end-users. Hospital management system, social networks, nuclear plant control system are just a few examples of Information Systems. They all have in common the fact that they receive data as input, process it and produce results in different forms.

An IS can be described along five dimensions that all participate to its operation: hardware, software, network, data, and personnel.

At the hardware level, electronic components offer low-level services only: a processor (CPU) executes elementary instructions, without the notion of computer program, a hard disk stores blocks of data without the concept of file, a network card emits electrical or light signal on a medium, with no knowledge of the application-level protocol that triggered the exchange.

Software activates and orchestrates these low-level services into more advanced functionalities that are truly useful and meaningful for the organization or IS owner. It is thanks to software programs that abstractions like a file, a transaction, a health record, a bank account exist and are managed by IS.

The network allows the IS components to exchange information through various protocols and media. Example of media are copper cable, fiber optics or electromagnetic waves; protocols allow to browse the web[3], to send email[4], convert domain names to IP addresses[5], control the status of devices…

Data is a central artifact, which is either consumed or produced by an IS, whose main purpose is to acquire data from its environment, to process it and produce results, that in turn can be new data or actions on the outside world, for instance in the case of Internet of Things actuators.

[3] HTTP protocol – Hyper Text Transfer Protocol.
[4] SMTP protocol – Simple Mail Transfer Protocol.
[5] DNS protocol – Domain Name Service.

Acquisition, hosting, operation and management of an IS require important financial and human resources, that are sometimes hard to find and lead to expensive costs. This paved the way to delegation or outsourcing of the management of part or all the Information System. This trend culminates in what is known as 'cloud computing', which makes IS services available through the network running on a technical infrastructure operated by a third party company, organized to deal with extremely high volumes of activity and to react to customer requests in a fast and fully-automated way, while offering comparatively low costs. The cloud approach allows to delegate the control on various IS levels, ranging from the infrastructure to the full service, including software development tools allowing customers to create and run their own applications. Today's Internet is full of 'as-a-Service' offerings, showing how important and impactful the outsourcing process is. Beyond the common 'Infrastructure as a Service – IaaS', 'Platform as a Service – PaaS' or 'Software as a Service – SaaS', indicating respectively outsourcing of the infrastructure only, of the development tools or of the full application, many other services are now offered for delegation, like 'Security as a Service', 'CEO as a Service', 'Blockchain as a Service'…

It should be clear by now that the structure of an IS can be very complex, with many parties involved. Assessing its security requires a proper mapping of its components and the identification of manipulated data and executed processes. This information can then be confronted with the security requirements of the IS, to verify that they are adequately met.

1.2. Defining security

The security of an Information System is qualified as non-functional requirement. It means that it does not directly affect the nature of the services, but rather the way they are offered. This explains the frequent relegation of security management to a concern of secondary importance, due to a pressure coming from the business to deliver in an increasingly quick way, imposing deadlines that are incompatible with a proper management of the system's security[6].

The security of an IS is not an absolute notion and needs to be defined according to security criteria. Requirements differ from system to system, and it is up to each organization or individual to identify the relevant criteria and evaluate its exact needs, otherwise being exposed to insufficient protection.

[6] Other reasons can also lead to unsecure systems, like lack of awareness or skills for instance.

Classically, three security criteria are considered, known as the CIA triad. ISO 27000:2018[7] defines them as follows:

- **Confidentiality** is "the property that information is not made available or disclosed to unauthorized individuals, entities or processes". It is concerned with making the information available to authorized eyes only.
- **Integrity** is "the property of accuracy and completeness". Integrity guarantees that information has not been modified by an unauthorized entity and is thus an exact image of the reality.
- **Availability** is "the property of being accessible and usable on demand by an authorized entity".

Beyond these three criteria and motivated by an increasing regulatory pressure and need for investigation, a fourth objective is often added, to describe the **traceability** of the IS, i.e. the ability to identify the entity at the origin of an event or an action. This also meets the need of **accountability**. **Non-repudiation** indicates the "ability to prove the occurrence of a claimed event or action and its originating entities". It goes one step further traceability by requiring the traces to be probative.

Analyzing the security of an IS ultimately boils down to identifying the relevant *security criteria* for all its components and defining the precise *level* of requirements for all the retained criteria. In some cases, confidentiality will be the most important criteria, while availability could be less demanding. In other cases, maintaining absolute integrity of information will be vital, while other situations could accommodate data corruption, as long as it can be detected and corrected. A hospital IS is likely to have more stringent requirements in terms of availability than a school's.

It is thus a two-fold analysis that should be conducted, the first one regarding the security criteria and the second one related to the level of requirements. This information will allow to define the right security posture that will adequately protect the IS. A poor choice of criteria or level will lead to an under-protected system, with potentially devastating consequences on the organization, or to an overly secured IS, causing needless costs and negative impact on the system's usability.

An information security incident is "a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security[7]".

[7] ISO 27000:2018 Information Technology – Security techniques – Information security management systems – Overview and vocabulary.

Companies, public organizations and bodies or private individuals are all equally exposed to security incidents and their potentially serious consequences, which can be of different kinds:

- Financial cost, due to the service disruption (loss of income) or time to repair the system (for instance after a ransomware attack);
- Intellectual property breach, like in case of compromised business secrets;
- Reputation of the organization, and by domino effect, impact on the trust of the public, the users or the shareholders;
- Non-compliance with the legal or regulatory constraints, for instance in case of data breach;
- Permanent loss of data;
- Physical harm to hardware;

In the most serious cases, a security incident can put a definitive end to the organization's activity. It is thus vital for it to properly identify the threats to its IS and elaborate a security plan to adequately and efficiently protect itself.

1.3. Threats and attack vectors

As described above, an Information System is a complex assembly of technical, organizational, and human elements that altogether contribute to the fulfillment of a functional mission. The IS is exposed to various threats that can impact its behavior, its data and its security as a whole.

A distinction can be made between environmental threats (natural disasters, floods, earthquakes, etc.) and human threats, whether accidental (handling errors, etc.) or deliberate (intrusion, malicious software, etc.). Threats can also be classified as internal (disgruntled employee for example) and external (competitor, hacker). Regularly, security incidents reported in the news show how powerful these threats can be, whether they originate from criminal organizations, states or economic powers.

To exert its effects, a threat exploits a weakness in one or more of the system's components. Whether it is an employee whose trust can be abused and provides access to the system, or a hard disk that is not duplicated and breaks due to heavy and long usage, or poorly designed, poorly developed or poorly tested software whose functionality can be abused, or the absence of written procedures that renders the response to an incident ineffective, all of these vulnerabilities are potential vectors of attack that could, when exploited, affect the security objectives of the IS. Threats and their attack vectors should be identified and addressed.

To do so, it is common to rely on the different dimensions of the IS described above, and to consider the possible vulnerabilities exposed by the components belonging to these dimensions. Depending on the axis considered, different vulnerabilities may be uncovered.

- Hardware axis: we consider breakdowns, wear and tear, sabotage, environmental threats, physical intrusion, theft, fire, power supply or connectivity problems...
- Software axis: as an engineered 'product', software is rarely free of vulnerabilities. This is demonstrated by the numerous patches published by software companies, aimed at closing security holes. These vulnerabilities (or most often a combination of them) can be exploited by malware[8] to spread or by hackers seeking to compromise or alter information. Depending on the type of software, the technologies used, the modes of deployment, the attack vectors differ, whether it is code injection, configuration errors, poorly designed or broken authentication, or authorization mechanisms[9]. Their exploitation undermines system availability and the confidentiality and integrity of its data.
- Network axis: communication within the IS and with its environment requires an efficient network. Whether private or public, such as the Internet, a network is a complex assembly of physical components (antennas, switches, firewalls, monitoring and control systems, etc.) and software (broadcasting, routing, quality of service protocols, etc.). It is possible to influence its operation, for example by modifying its routing rules (causing congestions or network partitioning), compromising name resolution[10] or address distribution; it is also possible to flood the network with traffic so as to prevent it from responding to legitimate requests[11], or to intercept or even manipulate communications. These attacks affect the availability, integrity and confidentiality of transmissions.
- Data axis: intangible but central component of an IS, data is exposed to irreversible disclosures, alterations or losses, following the exploitation of one of the above-mentioned flaws. The absence of access control, proper classification, back-up procedures, integrity verification codes and encryption are all vulnerabilities that can impact the availability, confidentiality, and integrity of information.

[8] A generic term covering various types of malicious software like viruses, trojans, worms, rootkits…

[9] The OWASP Foundation (Open Web Application Security Project) is a non-profit organization that regularly publishes the list of the Top Ten web application vulnerabilities.

[10] Domain Name Service – DNS.

[11] Denial of Service (DoS) attack or Distributed Denial of Service (DDoS) attack.

- Personnel axis: although its importance is often underestimated, the 'human' component of the IS is nevertheless essential to ensure effective and operational security. Indeed, Information Systems are designed, developed, implemented, executed, maintained, and used by human actors who may also have weaknesses: lack of awareness or training, sensitivity to manipulation or corruption, absence of rules or procedures are all elements that make the human being confronted with the IS risk not to act in the interest of its security, and thus to undermine its security objectives.

The vulnerabilities of an information system are potentially numerous; identifying them and taking corrective measures can be very complex and require multiple and specialized skills from various disciplines. A methodical approach should be followed to map the IS and identify the vulnerabilities as thoroughly as possible. This is the subject of the following section.

2. A risk-based approach for managing security

Securing an information system is a process that must meet various criteria:

- comprehensive: all components of the IS must be analyzed, and all potential flaws must be assessed and closed, if necessary. The most comprehensive analysis possible must therefore be carried out, otherwise the system will be inadequately protected, leaving open doors to attacks;
- integrated: limiting the IS to its IT aspects would reduce it to a mere technical reality and would deny its integration within an organization, for whose needs it was designed and operated. A security approach must therefore take into account the entire context of the IS, its place and alignment with the organization's strategy, as well as its organizational, human and contractual aspects. In the same way, security solutions must go beyond the sole technical framework and include organizational and regulatory measures;
- continuous: an IS is a system that is constantly evolving, whether due to changes in its environment (disappearance or appearance of technologies, new regulatory constraints, new organizational needs) or internal changes (error corrections, new operating procedures). It is therefore necessary to regularly reassess its security needs and its level of protection against threats to ensure alignment with the overall strategy of the organization.

A risk-based approach meets these criteria. It is the approach most commonly adopted to manage the security of an IS, which involves assessing the risks to which it is exposed, and proposing and implementing an action plan, while taking into account the organizational context. Whether it is the 'Risk Management Framework[12]' proposed by the American National Institute of Standards and Technology (NIST) or the standards from the ISO 27000[13] family published by the ISO (International Organization for Standardization), there are numerous reference systems that allow a structured, reliable and effective approach to be adopted in a variety of contexts, from small businesses to multinationals, whether you operate in the financial, healthcare or associative fields, by placing the concept of *risk* at the center of the analysis and action plan.

In order to define the notion of risk, it is necessary to introduce the concept of *asset*; by this term is meant anything that has value for the organization. It can be a process or information, but also technical or operational elements.

The first category covers the organization's *primary assets*; these are abstract elements that relate to the organization's missions and values. The second category includes the so-called *support* or *secondary assets*, which include all the components of the information system that contribute to its proper functioning and the proper management of primary assets. These include hardware, software, network, but also people or hosting infrastructures.

There is a direct dependency from the primary assets towards the secondary ones. A business process is supported by technical parts of the IS, managed by people, hosted in facilities. Similarly, information (patient data for example) is scattered over various storage devices, under the responsibility of persons, managed according to organizational rules. Attacking secondary assets has a direct impact on the related primary assets.

Threats target asset's security needs. By exploiting a *vulnerability* of an asset (typically a secondary asset), they reach primary assets, causing damage to the asset owner. Exploitation of a vulnerability happens with some *likelihood*, which depends on the ease of exploitation but also on the motivation and resources of the threat.

[12] https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview.

[13] https://www.iso.org.

If the security of an asset is affected[14], there are *consequences* or *impacts* for the organization. In the context of information security, these impacts are always negative, and can be associated with a level of *severity*.

To summarize, a risk scenario can be defined as the exploitation by a threat of a vulnerability leading to consequences. The risk can be defined as

*risk = threat * likelihood * severity*

Risk analysis is the "process to comprehend the nature of risk and determine the level of risk[15]". The level is based on the severity and likelihood of the risk scenario.

Risk analysis[16] is comprised of two steps: *risk identification*[16] and *risk estimation*[16]. The first one consists of identifying relevant threats, dreaded events and their consequences. The second one aims at measuring the level of the risk, by estimating the likelihood of the identified risks scenarios and the severity of the associated consequences. The result is a list of quantified risks that serves as a basis for prioritizing the risk selection and the risk treatment.

Risk treatment criteria have to be defined prior to the risk analysis, to establish rules for distinguishing acceptable and unacceptable risks. Risks of the first type are left as-is, while a risk treatment plan needs to be elaborated to deal with the risks in the second category and bring their level down to an acceptable one. Filtering the list of estimated risks to retain the ones that have to be mitigated is called *risk evaluation*[17].

The overall process of risk identification, risk estimation and risk evaluation is called *risk assessment*[17].

There are four common options for mitigating risks; they do not prescribe concrete measures, but rather define a general approach to deal with the risks deemed as unacceptable. The treatment options are the following:

- retaining the risk means that although the risk has been quantified as unacceptable, the organization makes the informed decision to accept it as-is;
- avoiding the risk means that the organization refuses to take the risk and thus eliminates the activity that gives rise to the risk;

[14] See section 4.

[15] ISO 27000:2018 Information Technology – Security techniques – Information security management systems – Overview and vocabulary.

[16] As defined by ISO27000:2018.

[17] As defined by ISO27000:2018.

- modifying or reducing the risk means lowering the level of risk to bring it into the acceptable zone. Reducing the risk can be done by acting on two factors: the likelihood of the risk scenario and the severity of its consequences;
- sharing the risk means that the risk is partially transferred to a third party, as is the case with an insurance or risk financing contract, where the third party agrees to bear the consequences of the risk.

Based on the retained option, a concrete plan of security measures is elaborated and implemented.

Another important step in a risk management approach is risk acceptance. Once unacceptable risks have been identified and a treatment plan has been established, the residual risks, i.e. the level of risks that remains after security measures are applied, have to be evaluated, to ensure they fit in an acceptable level. The organization's management must then formally approve the treatment plan, the decisions made and the residual risks. This step is important in that it engages the responsibility of the management and demonstrates its commitment.

Communication is a critical aspect in risk management. To properly assess the risks, it is essential to communicate with all stakeholders[18] to make sure the process is complete and efficient. It is up to business owners to identify assets, security requirements, severity of consequences; management must show its commitment to the process; technical people can provide information about vulnerabilities, attack vectors, likelihood. Communication does not only feed into risk management; it is also an outcome of the process, as the choices, decisions and measures taken as a result of the analysis need to be communicated, people need to be informed and trained.

Risk management must be operated in an iterative way. Periodically, the risks must be re-evaluated, to take into account changes that occur continuously in and around an IS, whether technological, legal or regulatory or business related. It is therefore mandatory to re-assess the decisions made in previous iterations in the light of the new context.

A generic risk-management framework is described in the ISO 27005:2018[19]. It provides guidelines for a risk-based management of information security, as described above, but in addition, it prescribes

[18] ISO 27000 defines the concept of 'Interested party'or 'stakeholder' as *a person or organization that can affect, be affected or perceive itself as being affected by a decision or an activity.*

[19] ISO 27005:2018 Information technology – Security techniques – Information security risk management.

the continuous monitoring and improvement of the risk management approach.

Different risk analysis methods exist, among others Mehari[20], EBIOS[21], CRAMM[22] or Octave[23]; all aim at assessing risks and establishing a mitigation plan for those deemed unacceptable. A mitigation plan is a list of measures, associated with cost, timeline and responsibilities that follow different lines of defense and cover the different dimensions of the Information System. Principles for establishing such plan are described in the next section.

3. Protecting the IS

3.1. Principles

When designing a protection plan, some generic principles apply:

- Security in depth: one line of defense is not enough; multiple layers of security must be applied, so that in case one fails, the next one will likely block the attack, and in case this second one fails, the attacker will hit the third one;
- No 'security by obscurity': one should not think that hiding a secret under the carpet will keep it protected. It should never be assumed that something that is hidden or obscure will not be revealed. Proper security mechanisms exist to protect information, and should be used;
- Least privilege: when associating privileges to an entity, always the minimal set of permissions should be granted, enough to ensure proper operations, but no more, or else run the risk of having him abuse the rights granted to him;
- Minimal trust: little to no assumption should be made by one IS component versus another. Everything needs to be checked: identity, format, type or size of data, environment, behavior…

Security measures must be defined along three main lines of defense:

- Prevention: every effort should be made to *avoid* a security incident. Preventative measures act on the likelihood of a risk scenario,

[20] Method developed by the CLUSIF (*Club de la Sécurité de l'Information Français*).

[21] Method developed by the French ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*) and Club EBIOS, the most recent version being EBIOS Risk Manager 2018.

[22] CCTA Risk Analysis and Management Method.

[23] Operationally Critical Threat, Asset, and Vulnerability Evaluation, developed by the Carnegie Mellon University.

by minimizing the attack surface and the number of vulnerabilities exposed by the assets. Running personnel awareness campaigns is an example of such measures;

- Detection: should prevention not be sufficient (and it is not), measures should be in place to allow for timely detection of security events. This means collecting, correlating, analyzing information at various levels and places of the IS to identify potential traces of security-related event, and trigger an appropriate reaction. Early detection minimizes the impact of a security incident. Anti-malware or intrusion detection systems are examples of detection measures;
- Recovery: when a system has been hit by an attack and suffered some damages, one must make sure he has the means to restore the system to an operational state, with minimal service disruption. Recovery also aims at reducing the impact. Examples of such methods are backups, that allow to recover lost data, or Disaster Recovery Plans, that establish plans and procedures to recover from a major security incident.

All three lines of defense must be present in a security plan: prevention is not enough, some measures may fail or become ineffective. It is thus mandatory to be prepared and able to detect any event that looks suspicious and may be the sign of an attack on the system. If the system is affected and its operation compromised, appropriate recovery methods are required. Missing any of these three lines of defense leaves the system poorly and inefficiently protected.

3.2. A layered approach

Following the 'defense in depth' approach, the security of the Information System requires attention along all different dimensions. In this section, we briefly cover main types of security measures applicable for the different axis of the IS.

Regarding hardware, the main concern is about its availability: here, measures primarily focus on keeping the system up and running, by using redundant components wherever possible to avoid single points of failure. Redundancy can be applied at various levels, from the single computer component to network elements, including power supplies, network providers, entire systems or even data centers, as is the case in a Disaster Recovery Plan. Physical access to hardware infrastructure is also key in ensuring its security. Procedures and documentation are also developed to preserve knowledge and allow for prompt reaction in case of incident.

Similarly, network infrastructure needs to be secured; components, paths also need to be redundant to avoid service disruption. Designing an

organization network follows an isolation principle, by logically or even physically separating the whole network in sub-networks, to limit and control the possible connections between zones, and avoid wide impact on the whole network in case a machine in one of the sub-networks gets compromised. Defining De-Militarized Zones (DMZ), setting up firewalls between the zones, monitoring the traffic to detect possible traces of intrusion are all security measures applicable to the network. Cryptography is used to ensure confidential transmission, also vouching for data integrity and authenticity, raising trust in some protocols.

At the (system) software level, focus is given to securely installing the software, limiting the attack surface by keeping the installed components to the minimum, hardening the installation to close any unnecessary access and make sure that the open ones are properly secured and monitored. Software update policy, anti-malware tools, backups are also key to securing the software platform. Intrusion Detection/Prevention Systems, Security Information Management (SIEM) systems, vulnerability assessments are key tools to assess and monitor the security of this layer of the IS.

Regarding the security of software development, measures are applicable to each and every step of the Software Development Lifecycle, from requirements engineering that need to also elicit the needs related to the security of the system, to architecture and design that has to define a solid structure, to programming that must follow secure practices, rely on proven existing tools and methods, to testing that not only has to check that the software delivered is functionally satisfactory, but that also from a security perspective, it is immune to all known attacks and interferences. Deployment is also critical, to ensure that the software is operated in secure conditions. Methodologies and tools exist that support the software engineering process.

Data, as the core business value, can be protected via various means, depending on the requirements. Cryptography can definitely play an important role: confidentiality can be accomplished by encryption, integrity can be achieved by using hashing techniques, authenticity is guaranteed through digital signature. Other techniques like steganography or watermarking can be used to embed secret marks in data and be able to trace down data leaks. Logical access control as well as backups are also key components of data security.

The last dimension of IS, namely people, may be one of the most important. Whether a user, a system administrator or an application developer, everyone has a role to play with regards to the security of the whole system. Although sometimes referred to as the ‘weakest link of security’, the

human factor can also be one of its allies. Running awareness campaigns, training sessions, raising skills and allowing time for tasks related to security, supporting, encouraging and showing appreciation from the management are all factors that, as a whole, take security to the next step in the organization.

An excellent source of information that can be used as a basis for both the evaluation or audit of the current security status of a system, and for structuring a security plan in response to a risk assessment, is provided in the ISO 27002:2013[24] standard. The document provides best practices to secure a system, grouping the proposed measures along 14 clauses (or sections) that address distinct areas of action, ranging from security policies to infrastructure protection, covering security in software development, systems operations or HR management… Each clause is split into categories that focus on a specific control objective and include a set of security measures meeting the identified objective. A total of 114 controls are included in the standard, also complemented with some implementation guidelines.

Conclusion

In this chapter, we went through an overview of what an Information System is, the threats it could be exposed to and the consequences it would face in case of incident. We then defined the security criteria that need to be considered when defining the system's security requirements.

In a second phase, we presented a key notion in security, which is the concept of risk. The risk together with its importance are the driving elements to define a security plan. We also described a generic approach based on international standards to assess the level of risk to which an organization is exposed, that it can rely on to elaborate and implement a security plan meeting its objectives. We insisted on the importance of adopting a recurrent, iterative approach, also aiming at the continuous improvement of the practices and processes.

Finally, we presented principles that guide the elaboration of a security risk treatment plan. Along the different dimensions of the IS, we described generic measures that help meet the identified and quantified security requirements.

[24] ISO 27002:2013 Information technology – Security techniques – Code of practice for information security controls.

Throughout this chapter, we referred to the ISO27000 family of standards and documents; the reason is that it is a widely recognized and adopted, continuously evolving set of repositories of reference information. It is also at the origin of other more concrete or focused methods that address only parts of the concerns described here. We thus consider it as a primary source of information and reference guide when it comes to defining, evaluating, and improving the security of an information system.

We would like to stress once again the key importance of the human factor when it comes to information security. A single weakness can have disastrous consequences, and it is the responsibility of everyone to avoid such scenario. Attacks are often complex, combining different vectors. Everyone has the power, by his attitude, skills, or mindset, to help prevent, detect or recover from a security incident. It is also everyone's duty.