III. ПРОБЛЕМЫ МЕНЕДЖМЕНТА И МАРКЕТИНГА. ЛОГИСТИКА

УДК 338.43

J. Neumeier, A.L. Zelezinskii, O.V. Arhipova

MANAGEMENT OF SECURITY OF INFORMATION IN COMPANIES

In the modern world, the problem of information security in companies is most acute, as the number of cyberattack attempts on company websites and domains has increased many times. There are many programs and developments that can solve this problem quite effectively. The article discusses an algorithm aimed at creating an information product aimed at ensuring information security at different levels.

Keywords: information security, algorithm, security, data storage security.

Ж.Нумьер[1], А.Л.Зелезинский[2], О.В.Архипова[3]

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КОМПАНИЯХ

В современном мире проблема информационной безопасности в компаниях стоит наиболее остро, так как многократно возросло число попыток кибератак на сайты и домены компаний. Существует множество программ и разработок, которые позволяют решить эту проблему достаточно эффективно. В статье рассматривается алгоритм, направленный на создание информационного продукта, направленного на обеспечение информационной безопасности на разных уровнях.

Ключевые слова: информационная безопасность, алгоритм, безопасность, безопасность хранения данных.

DOI: 10.36807/2411-7269-2023-2-33-38-41

Introduction

The management of companies covers many different aspects such as the company governance, the strategic conception, the management of people, deployment and handling of products, sustainable developments and so on.

The security of information being transversal within the whole organization of the company, its management is specific. The purpose of this article is to clarify how management of information and IT security works.

A vast majority of companies rely on known standards, especially for IT. Standards are described by norms handled by international or national organizations, one of the best-known being ISO. For instance, for project development, there is a norm ISO 21500 that defines projects key concept and that proposes methods to plan and conduct them. TOGAF is a set of norms helping to build IT architectures. More interesting for us and about security governance there is a series of standards called ISO 27000 introducing a number of concepts that I will take up in this article.

Before getting to the heart of the matter, let's introduce a couple of definition. An information system is an organizational system designed to collect, process, store and distribute information. It's made of essential assets and supporting assets. Essential assets are functions usually on a business level (e.g., to transfer money for a bank) or simply data (e.g. a bank ac-

[1] Нумьер Ж., аспирант Технологического университета Труа, г. Труа (Франция)
Neumeier J., Postgraduate of the University of Technology of Troyes, Troyes (France)
E-mail: jean.neumeier34@gmail.com
[2] Зелезинский А.Л., доцент кафедры менеджмента и маркетинга, кандидат педагогических наук, доцент; ФГБОУ ВО "Санкт-Петербургский государственный технологический институт (технический университет)", г. Санкт-Петербург
Zelezinskii A.L., Associate Professor of the Department of Management and Marketing, PhD in Pedagogics, Associate Professor; Federal State Budgetary Educational Institution of Higher Education "Saint-Petersburg State Institute of Technology (Technical University)", Saint-Petersburg
E-mail: uchposob@yandex.ru
[3] Архипова О.В., профессор кафедры гостиничного и ресторанного бизнеса, доктор философских наук, доцент; ФГБОУ ВО "Санкт-Петербургский государственный экономический университет", г. Санкт-Петербург
Arhipova O.V., Professor of the Department of Hotel and Restaurant Business, Doctor of Philosophy, Associate Professor; Federal State Budgetary Educational Institution of Higher Education "Saint-Petersburg State University of Economics", Saint-Petersburg
E-mail: olva@list.ru

count statement), that are "supported" by supporting assets (e.g., a server, a person, an application). Information security thus designate all the ways (e.g. technical, organizational, juridical) to secure essential and supporting assets, and therefore includes a scope wider than just IT.

ISMS

ISMS stands for Information Security Management System. ISMS helps to establish and drive a security policy in order to protect essential and supporting assets. Explained another way, its purpose is to set up actions (technical, organizational) in order to achieve an aimed security level. By analogy, the ISMS is the orchestra conductor that will drive security in the company. Its primary goal is to ensure confidentiality, integrity, availability and traceability of essential assets. The main functions of the ISMS are defined in the ISSP – Information System Security Policy. This high-level policy is strategic, and references lower-level policies.

The idea behind the ISMS is not just to achieve a state of security in the company, but to maintain it and make it last over time. The state of security is something that is not fixed and evolves, among other things over time. The power of computers is evolving and for example makes it possible to break encryption more quickly. New vulnerabilities are discovered every day on applications or components of the information system, which could allow malicious actors to enter the system. The political or geopolitical context can change, so attacks can focus on particular companies. Enterprises are "living" objects themselves, as the information system evolves over time. For all these reasons, security needs to be continuously integrated within the organization.

Continuous Improvement

ISO 27001 aims for continuous improvement of the system through a concept called Deming Wheel, also called PDCA cycle that consists of the perpetual reiteration of 4 phases:

1. Plan: Defining several levels of process and procedures, that put together will drive the ISMS – Information Security Management System.
2. Do: Operate the procedure and processes as planned in the first step. This phase is dispatched to several dedicated teams within the company (but not only) that:
   a. Either operates at an “operational” level, for instance by monitoring the security, managing users, collecting cyber intelligence, etc.
   b. Or at a “project” level, by accompanying the changes to improve the state of security step by step.
3. Check: This step aims to check whether there are deviations in the way the procedures are applied or not, and if the procedures do meet the security needs. In other words, if the "do" part is correctly operated and if the "plan" part is correctly calibrated. The "check" can be performed through audits, penetration testing, gap analysis etc.
4. Act: This phase aims to fill the gap identified in the "check" part through correction actions, by pushing changes to the "plan" and "do" steps.

Picture 1 – How to define the ISMS

Step 1: Define the scope

Prior implementing the ISMS, its scope must be defined by:

- Identifying what assets should be covered and
- Identifying the existing security measures that already cover them.

The scope chosen can be the whole company, but also a small part of it. Essential assets and supporting assets and their needs of security are listed during this step.

Step 2: Evaluate the risks

Once the first step is done, a risk assessment is performed on the scope previously identified. Vulnerabilities, threats, impacts, likelihood and finally levels of risk of the organization are identified. The way that the assessment is achieved is up to the company, as several methodologies exist, some are standardized other not. Whatever method used, ISO 27001 only sets out specifications to comply with. Among existing methods, we can cite:

- Probability/consequence matrix: This method consists of listing potential feared business impacts (e.g. impossibility to pay workers) and likelihoods of threat events on IT assets (e.g. a broken accounting software) to deduce and calculate risks (e.g. impossibility to pay workers *because of* a broken accounting software). For instance, EBIOS[1] method is based on it and is used extensively in France or Luxemburg.
- Delphi or ETE[2] method: Experts directly evaluate, identify and analyze risks based on both their expertise and a risk register that included potential risks and consequences. This method is often used when the scope of analysis is reduced because it is more efficient.
- Bow Tie analysis: Risks are identified based on known existing threat scenarios on IT assets and are then divided in potential contributing factors (vulnerabilities) and resulting business impacts.

Step 3: Treat the risks

Once all the risks have been identified, they must be dealt with. 4 ways to treat the risks exists:

- Avoidance: If an identified risk is unacceptable, or if the risk mitigation actions are easy to implement, a dedicated politic must me set up in order for the risk either to *never* occurs, or to have *no impact*.
- Reduce: The likelihood or the impact of the risk *is reduced* through technical measures at acceptable levels.
- Transfer/share: The responsibility of the risk is *transferred*, for instance by outsourcing its management, or by subscribing to an insurance.
- Acceptation: No measures are implemented, because the risk is accepted *as is*, usually either temporary or because the risk itself is minor or extremely low.

Residual risks that couldn't be lowered to an acceptable level must be subject to further measures.

Step 4: Choose security measures to implement

This last step consists to choose security measures among a register. ISO 27002 proposes more than 120 control points that are divided in 14 controls. The control points must be chosen based on the risk assessment, in order to comply with mitigated or accepted risks (as they might evolve) and non-mitigated risks.

The control points cover for instance the following topics: IS[3] policies, organization of IS, human resource, asset management, access control, cryptography, operations security, physical & environmental security, operation security, communication security, system acquisition, development & maintenance, supplier relationships, information incident management, IS aspects of business continuity management, compliance, IS incident, etc.

The selected control points should be covered by the ISMS and therefore serves as guidelines to build the underlying procedures and processes.

[DO] Improve and monitor Security

The "DO" part consists of the application of the guidelines defined in the ISMS on an operational level. This part can vary a lot from one company to another, dependently on their security needs, the control sets selected, and their budget.

As stated before, the application of security measures is dispatched to several distinct teams within the company, each operating on its respective perimeter. In general, companies embed thereafter functions:

- Identity Access Management. The role of IAM is to centralize the functions related to identity and accesses of users within the company. It is also to manage privilege access (e.g through technical accounts). IAM:
  - Handles a register of users that contains their access rights (e.g. what application a user can access) and their authorization (e.g. what a user is allowed to do within an application),

[1] EBIOS: In French: "Expression des Besoins et Identification des Objectifs de Sécurité" translated as "Expression of Needs and Identification of Security Objectives"

[2] ETE: Estimate-Talk-Estimate

[3] IS: Information Security

- Tracks departures/ arrival and periodically recertify rights (e.g. they check if users are still allowed to possess their rights),
- Operational Security or SecOps. SecOps involves dedicated teams using security tools to protect against risks. Operational security consists for example of:
- Incident monitoring and response (e.g. through antiviruses, data leak prevention & protection, security events monitoring, etc.),
- Planification of technical controls such as vulnerabilities scans on IT assets, of recurrent penetration tests, of configuration reviews, etc.,
- Cyber intelligence such as periodic reviews of new vulnerabilities and threats,
- Security Administration that aims to administer the security of tools / assets, by ensuring the:
- Management of secrets (e.g. generation / storage / management of passwords, certificates, public / private keys),
- Management firewalls (e.g. opening or closing network flows, refusal of requests to open unsecured flows, etc.),
- Management of platform security (e.g. maintenance of operating systems, applications or middleware through patches or updates),
- Governance & Risk Management that mainly support on projects to increase the level of security, for example through:
- Risk Assessment over every IT project in order to identify and mitigate risks linked, among other things, to non-compliance with the security policy,
- Purchase & outsourcing: third party risk assessments before contracting, reviews and insertions of security clauses in contracts,
- Security awareness: management of sessions to raise awareness of users.

When **not managed by a dedicated team**, security functions are handled by other entities as they can be **cross-functional**. For example, human resources apply checks when staff arrive, IT architects include security requirements in their specifications, etc.

Check and act:

The "check" steps consist of detecting changes or gaps with the ISMS governance, as well as improvement needs. Enterprises embed 3 tools to achieve that:

- The internal control, that checks if process and procedures work correctly and are followed.
- The internal as well as external audits (including penetration testing) that checks the performance and the compliance of the ISMS.
- The reviews (or re-examinations) of the ISMS which periodically guarantee the adequacy of the ISMS with its environment and the current information security needs.

Finally, the "act" step consists to implement corrective, preventive or improvement actions as a response to incidents or discrepancies observed during the "check" phase and thus prepare for the next cycle.

Conclusion

The management of information security in companies represents a very significant cost, due to the extent of knowledge, resources in terms of personnel as well as the tools necessary for its application. It is particularly critical for companies with a low budget but high security issues. Nevertheless, the ISMS concept is meant to be adapted according to the company's context, and the budget for security is often justified in view of potential impacts. In Europe, in 2022, the median budgets spent on cybersecurity in large enterprises amounted to US$2 million (compared to $6.77 million for the IT department in general) while SMEs[1] invested $150,000 (compared to $375,000 for their IT).

References

1. Joyce, Sean, "C-Suite Cyber Playbook", PWC, 01/01/2023, pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights (accessed the 11/03/2023).

2. ISO/IEC JTC1/SC 27 technical comity, "ISO/IEC 27000:2018", ISO, 01/08/2018, www.iso.org/fr/standard/73906 (accessed the 11/03/2023).

3. Indeed Editorial Team, "5 Risk Analysis Methods and How to Use Them", Indeed, 11/03/2023, www.indeed.com/career-advice/career-development/risk-analysis-methods (accessed the 11/03/2023).

[1] SME : Small and medium entreprises