AARMS Vol. 17, No. 3 (2018) 171–178. **10.32565/aarms.2018.3.12**

Seven Pieces of Advice to Improve Your Information Security

Best Practices from the Enterprise's Point of View[1]

Gergely SZENTGÁLI[2]

Establishing and operating an effective information security management system within an organization is never an easy job. Organizational culture, management support, budget restrictions and many other factors affect the security efforts of a company. Although the information security academic literature is growing, there is no clear guidance in several fields of the topic, therefore the life-tested best practices can be a useful aid in operating such systems. The aim of this paper is to provide a short guidance regarding the basic steps of a beginner information security manager, and maybe to give some useful thoughts to the experienced officers, as well.

Keywords: *information security, ISMS, cyber security, risk, incident, management*

Introduction

Information security practices and methodologies are evolving every day. The threat environment is constantly changing, forcing the companies and security professionals to learn, improve and adapt. There may be a lot of differences between the public and private sector, still I believe that the following information security practices can be used on both sides. In the following, I am going to introduce seven pieces of advice regarding information security which are coming from my managerial and auditor experience, serving as a guidance for a minimum standard what every information security manager should do in order to improve their organizational defence capability, and to review their taken steps to achieve this goal.

Don't be a Lone Wolf: Gain Management Support

Supporting and auditing companies worldwide, my experience was that the common reason of failed information security management systems (ISMS) was the lack of senior management support. Information security managers who are trying to build and operate ISMS without management sponsorship will find themselves alone. However, gaining

[1] Edited version of a presentation in *Cyber Security in Public Sector* international scientific conference.

[2] Information Security Manager, IT Services Hungary; e-mail: gergely.szentgali@t-systems.com

the management's approval is not easy: the information security manager has to make the board understand why security is so important.

The members of the leadership of companies talk a unique language, the IT jargon should be avoided if you communicate to them. The regular root cause of miscommunication is that the members of the senior management are usually not IT experts, and the security manager is not a business leader. It is not easy to bridge the gap between the strategic priorities and day-to-day operational governance concerns: the board is focusing on brand reputation, financial revenue and business objectives, whereas the (security) governance is dealing with daily challenges. [1] Therefore, in order to fill this gap, one of the mandatory elements of the General Data Protection Regulation (GDPR) is the basic information security education of the board members. [2]

Using a business case, including cost and benefits (not just financial), to present your ideas is always a good choice. Let them know that the IT and the information security itself are serving the business, and your goals are always aligned with the objectives of the business.

To achieve success, you have to involve the proper stakeholders: explore and draw your stakeholder map, get familiar all the "players" within your organization. Involvement has many aspects: organize steering committees, security meetings and maintain reporting channels. With a well-established relationship between the board members and the information security manager, many security incidents can be prevented and the budget of the security program can be secured year by year.

Know Your Next Steps: Implement a Security Strategy and Governance

Knowing that the management supports your efforts, you should have a vision and a structure to achieve your goals. Without a clear target, even a brilliant strategy will fail. Creating an information security strategy will guide you and your employees regarding how to achieve the desired state. Be realistic, set up accountable, and—maybe it is the most important—measurable goals. Use key performance indicators (KPIs) in order to track your progress.

The well-established governance structure comes from a proper strategy and the connecting policy. Compliance to the policy and policy changes is always a challenge. Employees resist changes in most cases, and this noncompliance results security risk. An information security policy should be enforceable, but still, the communication and popularity of the security policy has to be the cornerstone of the ISMS: a positive attitude toward a mandatory security change leads to greater intention to comply. [3]

Regarding the governance structure, build up information security roles depend on the size of your organization, such as Chief Information Security Officer (CISO), Business Continuity Manager, Chief Data Privacy Officer, security administrators, and so forth. Due to the defined roles, accountability and separation of duties come true, and it will be also helpful to create and maintain escalation channels. Through the identifying the process and data owners, proper asset classification and the level of the linked controls can be successfully determined.

The information security governance system should be led by the CISO who is ideally directly reports to the Chief Executive Officer. In some cases, the Chief Information Officer can be the direct supervisor of the CISO. A well-trained and experienced information security team is important in such structure, and operates as a consultancy and guidance point for the business. To achieve this goal, the team should be visible and reachable from the business functions, what can be done if information security is a respected value and priority of the organization. [4] A well-built information security management system is transparent, hierarchical, understandable and executable for every employee.

During building up your governance system, do not be afraid to use international standards and best practices. You do not have to reinvent the wheel, there are several good solutions what you can use. For an example, ISO 27001 standard[3] [5] is a cornerstone of today's ISMS, supported by many others, such as ISO 22301 for business continuity management, [7] or ISO 31000 for risk management. [8] One of the biggest advantages of using an international standard is that your organization can be audited and certified. This is a clear statement for the outside world, and also can be a contract requirement from the customer's side. Regarding IT service management, besides ISO 20000, [9] ITIL [10] can be a reliable source, even only some part of it: if your organization is focusing on IT system operation and you are facing budget restrictions, than implement just the operation phase of the IT service lifecycle.

See the Big Picture: Use a Tool

A tool, which here means a software, can make the information security manager's life easier with providing dashboards, tracking status, maturity level, etc. With a universal product, you are able to manage your audits and track the findings; record the results of risk assessments; perform a business impact analysis; set up a strategic program management and many more.

The IT security market is growing, and new products appear every day. Besides antivirus programs, firewalls, intrusion prevention and detection systems—information security management software should be also the part of a security management's portfolio. Since every organization is different, the tuning and tailoring capability (e.g. self-releasing) should be a primary condition of such product.

The reports produced with this tool can be a status snapshot, identifying the strengths and weaknesses, and also fits for audit purposes: the internal or external auditor can get a picture quickly on the organization's maturity and compliance compared to the chosen standard. In the age of GDPR, this capability will worth to invest in, but will be helpful for those who are out of the GDPR's scope, as well. The senior management can also require risk management status, or compliance reports.

As an example, Figure 1 shows a spider graph regarding an organization's ISO 27001 maturity and compliance.

[3] The number of ISO 27001 certified entities is growing every year, in 2017 more than 39,000 organizations were holding this certificate. [6]

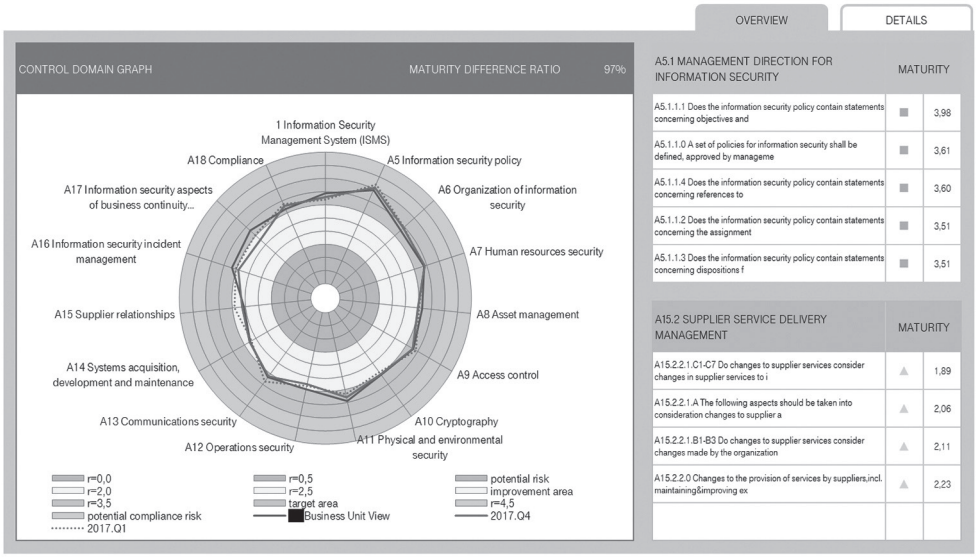

Figure 1. *Spider graph of ISO 27001 maturity with the highlight of the strongest and weakest fields.* (Screenshot by the author from [11].)

This spider graph is made with a few clicks, and operates perfectly for showing the current status of ISO 27001 compliance. The graph can be created for every international standard, or even customer requirements which are uploaded in the system as a control assessment.

Focus on the Whole Lifecycle of Risks and Incidents: Tracking is the Key

Performing risk assessments periodically is one of the basic tasks of an information security manager. Exploring the new threats is the first thing to do in preparation for protecting the organization's information assets. As in so many other cases, there are no new tricks on the field of risk management, as well—you have to follow the classic lifecycle: identification, analysis, evaluation and treatment. [12] A tool—mentioned in the previous chapter—can be a useful ally regarding the tracking of your incidents and risks. This is a core point, because in several cases, the information manager is just opening the ticket, but does not manage it through, losing the possibility to see the big picture and find connections between events. It is also the information security manager's overall responsibility to maintain the risk and incident database.

Always give time for post-incident reviews. In most cases, after analysing the root cause, the risk can be eliminated and the incident can be closed for a lifetime. Involve the stakeholders, give time for a brainstorming in order to improve your security. Inform your management about the improvements and the current threat status. Always be honest, do not play with the numbers—transparency is a long-term basis of management sponsorship.

Get Comfortable with the Uncomfortable: Test Yourself and Be Prepared

Incident management is a core activity of information security management. The preparedness, response time and tools are vital parts of the survival capability of an organization. It may happen that your company's daily operation or even its reputation will depend on how good your readiness is.

As an information security officer, it is your responsibility to create, maintain and test your incident management plan and processes. You have to train your colleagues, test their knowledge and preparedness. Do not underestimate the utility of incident management exercises. Drills and regular tests will create reflexes which pay off in a stern situation.

Build up your own incident management team. Resourceful companies are able to operate a Computer Emergency Team (CERT) or a Security Operations Center (SOC), working in 24/7, employing IT security experts in shifts. But money cannot be an excuse: take your organization's head of IT operation and a technician from that department, an IT technician with security experience, somebody from the management (with the right to make decisions), a communication expert, train them, build up escalation channels and procedures, and your very own incident response team is ready. Of course, it will not be equal with an SOC or a CERT, but an information security manager has to adapt to the limits of the organization. You have to win the management for the cause because in the long run it will not be a solution due to the rising number of cyber-attacks, and the fact that lots of roles have to be shared among less people. [13]

Business continuity and disaster recovery strategies, plans and scenarios also should be tested on a regular basis. It does not matter if you are working for a bank or in the public sector, service outages can cause financial and reputational loss, and in some cases can escalate into a national security risk, as well. When the time comes, success will depend on your employees' preparedness. Just like on some other fields of information security, during the creation of these plans, the business (especially the business process owners) should be deeply involved since the requirements are coming from their side.

Communication and its channels are vital. In case of the public sector, it has to be a must to maintain an active dialogue between the organization and the Government Incident Response Team (GovCERT) since its basic task is the incident handling of central and local government agencies. [14] It is not only essential for the updated information, but to reach the GovCERT as quickly as possible in a case of a serious and/or high priority incident. Communication plays a central role in public relations (media, customers, etc.), your organization should be prepared for crisis communication: train appointed employees to communicate to the media in order to control the situation.

Strengthening the Human Factor: Security Awareness

It became a cliché, that the weakest link in information security is the human factor, the user itself: high percentage of successful attacks is starting with social engineering. Moreover—according to the IBM 2016 Cyber Security Intelligence Index [15]—60% of attacks came from the inside, showing clearly that insider threats continue to pose the most significant

risk to organizations.[4] Despite the international trend, employees believe information security attacks are external factors, therefore do not consider themselves a threat. [17]

A trained employee is the first line of defence in protecting the company's information assets. With a well-established awareness program, a person's awareness becomes a (preventive and detective) control. The goal of the awareness activities is to make the employees understand the importance and implications of information security, moreover the safe behaviour, aligned with the organizational information security policy. [18]

These kinds of trainings should be mandatory in online or in-door form. After you identified the needs and goals of your organization, create a steering committee to assist in planning, executing and maintaining the awareness program. The information security strategy will be a compass to understand the connection between awareness targets and business objectives. Shaping the awareness program, you should focus on four domains: people (the right employee in the right role), technology (up-to-date technology with implemented security features), processes (role-based and effective), and policies (clear and high-level statements). [19]

Tailor your training to your audience, use everyday examples for better understanding. In addition to trainings, there are many other practices for raising information security awareness: posters, intranet news, e-mail campaigns, etc.[5] The goal is to make the employees understand: security is not just a management issue, security is everybody's business. The final goal is to organize the quickest training possible that has the greatest impact on target groups. Use your employees and the awareness steering group to review your program at least annually.

The result of an awareness program should be tracked and tested on a regular basis. Controlled phishing campaign, fake calls and many other tests will prove the awareness level of the organization. After this, the information security manager has to communicate and explain the results for all the employees. In lessons learned sessions, they have to understand what would happen in a real-life situation. Facing the actual consequences is one of the best methodologies to shape a user's behaviour.

And Finally: Be Emphatic

Be emphatic, because sometimes security can be viewed as a burden: most of the employees consider security controls a nuisance and unwanted obligations. Every security officer knows the typical questions: "Why do I have to change my passwords again?" or "Why do I have to keep my desk clean?" Such questions usually lead to uncooperative attitude.

---

[4] Regarding insider threat we have to make difference between the malicious insiders and inadvertent actors. In the 2016 IBM report, behind the 44.5% of the 60% attacks were actors with malicious intent. However, in the latest, 2018 IBM X-Force Threat Intelligence Index [16] considers insider incidents as hot topic, as well. The report concludes that in the age of bring-your-own-device, everyone is an insider threat, and the errors of inadvertent employees (e.g. weak passwords, unsecured personal devices, etc.) could lead to serious security incidents.

[5] Alternative solutions can provide cost-optimized tools for smaller organizations. Being creative is the key regarding an awareness campaign. Focusing on such methodologies could change the current trend which shows that big size companies (with higher security budget) have higher awareness level, while the smaller ones have lower. [20]

The solution is the engagement: just like in case of the senior management, employees have to understand why security and their participation are important.

Starting from their first day at the office, employees should be trained regarding security. Help them with easy-to-understand materials, for example create a one-pager from your information security policy or rule base. As I stated before, employees' compliance to the security policy often fails, and in several cases, it comes from the size and the poor structure of the document. Nonetheless, security policy has to be the basis of the ISMS; still there is no clear guidance on how to design such a document. However, at the end of the day, it is the information security manager's responsibility to make the security policy a useful tool for the organizational governance and employees, as well. [21]

Motivate your employees through awards for their awareness, e.g. after a successful clean desk audit. Make good practice as an example to follow, and spread via the organization's communication channels such as the corporate intranet.

Working as a security manager will give a very specific perspective on your organization, but it still remains just one point of view. Therefore, require input from employees regarding information security, because sometimes they see better the everyday risks and potential threats in their personal environment. It is worth making exit interviews in order to reveal what kind of failures they have seen in the organization's information security system during their employment.

Summary

Discussing minimum information security standards is always subjective. In this paper I summarized and aligned with my experiences seven pieces of advice to improve your information security, but this is a highly personal point of view. An information security manager should be aware of the changes in this field, train himself/herself and always be ready to respond to the upcoming threats and security challenges. At the end of the day, the senior management has to understand the importance of information security, and with the support of a security team, the business and security goals can be achieved.

There is no hundred percent security, so this cannot be the final goal—a well-configured ISMS' aim is to manage the risks on an acceptable level. As I stated before, you do not have to reinvent the wheel: methodologies, tools and best practices are public and available. It's your turn now.

References

[1] KELLY, T. S.: Building Bridges with the Board—Innovation in Information Governance. *ISACA Journal*, 3 (2018), 34–38.

[2] TÓTH, A.: Future Information Security Threats to the Defense Sector. *Hadtudományi Szemle*, 10 4 (2017), 246–257.

[3] BÉLANGER, F., COLLIGNON, S., ENGET, K., NEGANGARD, E.: Determinants of early conformance with information security policies. *Information & Management*, 54 7 (2017), 887–901. DOI: https://doi.org/10.1016/j.im.2017.01.003

[4] THARAKAN, D. J.: Protecting Information—Practical Strategies for CIOs and CISOs. *ISACA Journal,* 3 (2016), 34–36.
[5] *ISO/IEC 27001:2014 Information technology—Security techniques—Information security management systems—Requirements.*
[6] CHARLET, L.: *ISO Survey 2017.* www.iso.org/the-iso-survey.html (Downloaded: 06.01.2019)
[7] *ISO 22301:2012 Societal security—Business continuity management systems—Requirements.*
[8] *ISO 31000:2018 Risk management—Guidelines.*
[9] *ISO/IEC 20000:2005 Information technology—Service management.*
[10] *What is ITIL Best Practice?* www.axelos.com/best-practice-solutions/itil/what-is-itil (Downloaded: 05.10.2018)
[11] avedos *risk2value* software, special release for T-Systems International GmbH.
[12] SZÁDECZKY, T.: Risk Management of New Technologies. *Academic and Applied Research in Military and Public Management Science,* 15 3 (2016), 279–290.
[13] HÁMORNIK, B. P., KRASZNAY, Cs.: Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics. *Academic and Applied Research in Military and Public Management Science,* 16 3 (2017), 73–92.
[14] FEHÉR, J.: Incident management of central and local government agencies. *National Security Review,* 2 (2016), 78–92.
[15] IBM: *Reviewing a year of serious data breaches, major attacks and new vulnerabilities. Analysis of cyber-attack and incident data from IBM's worldwide security services operations.* www.autoindustrylawblog.com/wp-content/uploads/sites/8/2016/05/IBM_2016-cyber-security-intelligence-index.pdf (Downloaded: 23.05.2018)
[16] IBM: *IBM X-Force Threat Intelligence Index 2018. Notable security events of 2017, and look ahead.* https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-research-report-77014377usen-20180329.pdf (Downloaded: 03.01.2019)
[17] BAUER, S., BERNROIDER, E. W. N., CHUDZIKOWSKI, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security,* 68 (2017), 145–159. DOI: https://doi.org/10.1016/j.cose.2017.04.009
[18] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., ZWAANS, T.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security,* 66 (2017), 40–51. DOI: https://doi.org/10.1016/j.cose.2017.01.004
[19] DAHBUR, K., BASHABSHEH, Z., BASHABSHEH, D.: Assessment of Security Awareness: A Qualitative and Quantitative Study. *International Management Review,* 13 1 (2017), 37–58.
[20] SASVÁRI, P., NEMESLAKI, A., WOLF, R.: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Military and Public Management Science,* 14 1 (2015), 63–78. DOI: https://doi.org/10.1016/j.cose.2016.12.012
[21] KARLSSON, F., HEDSTRÖM, K., GOLDKUHL, G.: Practice-based discourse analysis of information security policies. *Computers & Security,* 67 (2017), 267–279.