White paper Information Security Management

November 2015, Géant SIG ISM
Author: Alf Moens
Review: Rolf Sture Normann, Andrew Cormack, Bart Bosma
Version 1.0

No longer is information security an area of ICT technology only. It is about protecting business operations, protecting assets of an organisation and interests of researchers, students and employees. Information security is an essential component of business operations and business continuity.

This white paper describes what the management of information security entails and how it can be implemented in an organisation.

This paper is about information security. Another term heard often is cyber security. It is used mostly in the context of Internet and cloud computing, usually as a umbrella term. In this paper we will use the term "information security", since non-technical activities and non-digital forms of information can also create significant risks.

History

Even before the era of computing technology there were serious reasons for protecting information. Since the days of Julius Caesar, and before, information has been regarded as a strategic asset that needs to be protected. Our present society cannot do without the massive flows of information. Various sectors are depending heavily on swift and correct data. Assuring that this information is available and that it is sound and trustworthy is the main goal of information security. To make this work, a mixture of disciplines and measures addressing technique, processes, knowledge and behaviour, is needed. Information security management ensures that this is managed in a balanced and continuous way.

Audience

This white paper is targeted at security professionals and senior information management. Although it is written for NRENs, it can also be used in other sectors and branches, since there are no NREN specific subjects. It can be used as a starting point for setting up information security management in an organisation as it covers all aspects of information security management. This paper is loosely based on the ISO standard on security management, ISO 27001[1]. However, it doesn't cover everything from this standard.

[1] ISO 27001 is an international standard that describes the information security management process, against which an organization can certify its security management system. ISO 27002 is an international standard that describes best practices for implementing information security in an organisation.

What is security management?

Security management is not a one time exercise. It is a continuous operation that needs to be embedded within the entire organisation. Security management deals with controlling the confidentiality, integrity and availability of information, information systems and infrastructure for an organisation. Security management is a continuous process with repeating steps of analysing, implementing, controlling and improving. You are never done. Every change, whether in the business, the rules and regulations, technologies or in staff, requires a regular evaluation and adaptation.

Risk management

Information security management starts with an inventory of the most important assets for an organisation, assessing threats and quantifying risk, and assigning responsibilities. Information security management then evaluates which measures to implement, enhance or improve, to reduce the risks to an acceptable level. Some risks are easy to counter, others are accepted (you just take the extra cost involved with an incident), and some are too big to handle by your organisation. In the latter case the organisation can decide to transfer the risk with extra insurance or terminate the activity that causes this big risk. There are several methods for risk analysis, risk methods and risk treatment. Choose one that is close to your organisations culture and habits. Beware of being too precise in quantifying risks and the costs involved with risks.

Initial Setup

Most organisations do not start from a greenfield situation. In most cases some measures are in place already, for instance there may be an incident response team (CERT/CSIRT), or even a security officer and a security policy. When setting up security management initially, it should be treated as a project with a beginning and an end, and with a clear goal. Once the setup is completed, there should be a continual improvement cycle.
Steps that should be part of the initial set up of security management are:

- Roles and responsibilities: Responsibility and accountability must be assigned clearly in the organisation. The CEO will always have the final responsibility, but usually will delegate security management to the security officer, which can be a role or a function. Next, each individual involved (employee, student, researcher, guest, contractor) is responsible for acting according to the company rules and regulations. Finally, responsibility for datasets and information systems and services needs to be addressed and assigned.
- Resources: Apart from roles and responsibilities the resources needed for these roles need also to be addressed specifically and ownership must be assigned. Most important is manpower and funding for external audits. If you are starting with the implementation and still need to build up expertise, having budget for consultancy will help to make a quick start.
- Determine your critical assets: This can be done by looking at the data stored and processed in the infrastructure and by looking at the business

processes (how do you make money?). Also, take into consideration what laws and regulations you have to obey for these activities.

- Risk inventory: After identifying your critical assets, analyse which threats are related to the assets confidentiality, integrity and availability.
- Standards and frameworks: Decide which standards and frameworks to use. Look for standards that are popular and common in your sector. Use something that is mainstream, there is a lot of material available. A framework describes how to set up information security management. The framework for information security used most often is ISO 27001. It can be used to certify your security management system. However, as long as there is no external need for certification, just use the framework to get your management system up and running.
- Guiding policies: guiding policies describe your information security rules and regulations in more detail. While a security policy describes the main topics in general terms, a guiding policy describes your implementation in more detail. A common pitfall is to produce a large number of guiding policies and impose them on your organisation, resulting in large sets of documents no one is using. Make sure your 'art of policy making' matches the experience and culture of your organisation and look for the right balance between policy detail and user responsibility. For maintenance reasons and for ease of use creating one large policy is not practical. It is good practice to create a number of smaller policies, at least including an acceptable use policy, a password policy and a mobile device policy.
- Baselines: A baseline describes how to implement information security in detail. Whereas a standard describes what to do, a baseline describes how to do it. Typically, there is a general baseline that describes how to implement the selected standard. Sometimes it is complemented with technical baselines for the configuration of servers, databases, workstations, and mobile devices.
- Awareness (website/intranet): The success of information security depends on the involvement of everyone working in the organisation or working with the organisation's information systems. In many cases security measures are seen as an obstacle and not as a necessary condition for operating a business. The goal and need of security should be explained on a regular basis. This can be done by training, promotional activities, information on websites and intranets, discussions in team sessions or, preferably, a combination of these. Creating support and understanding for security is the most difficult part of implementing security management, and the most neglected, but it is the key to success. Although you may be able to enforce certain measures, embedding information security in all business processes should be your ultimate goal.
- Incident response: No matter how well you assess risks and implement measures, there will always be incidents. Not one piece of software or hardware is flawless, and you will never be able to prevent mistakes, failure of components, or external threats. An incident response process allows you to address incidents quickly, assess the impact, prevent spreading or escalation, remediate possible damage, learn about

vulnerabilities and fix them. Incidents should be registered for follow up, analysis and reporting.
- Training: All personnel must be trained for security, although for most people this is covered in awareness trainings. However, some staff requires specific security training on a regular basis: security staff, incident response handlers, software developers, ICT purchasers (for cloud services and for outsourcing), network and systems management.

These steps are the major subjects to cover, but there are a lot more: Supervision and sanctioning, forensics, legal requirements, encryption technology, classification of data, technical baselines, mobile computing, personnel and contractor screening, baselines for cloud computing, information security in projects, and so on.

What about privacy?

In the mid 2010's privacy has become a boardroom topic, just like cyber security. Essential for compliance with privacy regulations is the protection of privacy sensitive data. This is where privacy and information security intersect. Privacy also imposes criteria for designing software and information systems with principles such as *privacy by default* and *privacy by design*. And, if your organisation stores and processes privacy sensitive information, and most organisations do, you should take the legal requirements of privacy regulations into consideration when doing risk assessments and assessing project proposals.

Security Management

When the initial setup is on its way, management of the process starts. This really should be started at the same time the initial set up starts, but certainly soon after the start once the initial responsibilities are clear. Security management consists of several management cycles. Typically, the security management process is 'managed' by the security officer:

- Monthly cycle: Although the term *monthly* is used, this cycle concerns day-to-day operations, monitoring daily security operations, and reporting on daily, weekly and/or monthly basis.
    - Monitoring daily security operations: in larger organisations security incidents will be handled by multiple people. Monitoring ensures incident handling is according to plan and follow-up is secured.
    - Escalation: Some incidents are more complex or require involvement of senior employees for other reasons. Some may need, because of the impact of the incident or legal ramifications, escalation to senior management or to the board.
    - Reporting: There are several reasons for doing regular reporting on information security. Most important are justification to management and other stakeholders and raising awareness. Depending on the number of incidents, the reporting cycle can be daily, weekly, monthly or a combination of these. Typically, there is a form of reporting concerning operational security issues and monthly management reporting. Serious incidents can result in

exception reporting and advisories for internal or sometimes for external.

- Improvement cycle: Based on the risk analysis and more detailed assessments on information systems or departments, improvement projects have been drawn and are executed throughout the year.
    - Awareness: plan for several awareness raising activities using different methods and targeting both the whole community and specific groups. Whether the message is scary or reassuring, make sure to always refer to a solution. Possible activities can be games and simulations, mystery guests, presentations and seminars, and so forth. Make sure that the message is repeated and that it is presented by different people in the organisation, for instance security specialists, board members, middle management, but also an incident response worker, a software developer or an HR consultant.
    - Improvement projects: improvement projects are defined and executed based on audits or assessments. For the most part they will be executed within departments. The role of security management is to guard goals, to make sure that results are met and to monitor the consistency of projects.
- Quality cycle: This cycle consists of yearly activities.
    - Risk assessment and auditing: both internal and external auditing. Pentesting could be part of integrated systems management, but could also be part of the audit calendar of security management. A form of an internal audit is the *management review*.
    - Evaluation of improvement plans.
    - Evaluation of policies, organisation of security, roles and responsibilities.
    - Management review: ultimately, (senior) management is responsible for a secure and safe operation. Management will be involved on a regular basis through monthly reporting and exception reporting. In addition, a formal management review should be performed at least once a year. During the formal management review management is asked to reconfirm they are committed to the security policy and the implementation of the policy, in fact the entire security implementation, is evaluated.

Standards

The information security standard that is used most often is ISO 27002, both in governmental environment and in semi-public and private businesses. Another standard and framework that is used often is COBIT. COBIT's aim is controlling systems and network management. Security is an integral part of it, although not described with as much detail as in ISO 27002. NIST has a lot of technical standards that can be used as technical baselines. PAS 555 is a new (2014) British high level standard describing the components of security management without going into detail. Its goal is to be a generic standard for use with different frameworks.
To use the standards mentioned above, you'll have to pay a small fee to compensate the standardisation body that maintains and distributes the

standard. There are also commercial initiatives for standards of which the ISF[2] Standard of Good Practice for Information Security is the best known. It is a membership based organisation aimed at multinationals; the materials are available to members only for a serious fee.

Furthermore, there are sector specific standards, some of which express the specific needs for a particular sector such as the banking sector, while others are implementations of international standards, translated to sector specific jargon, for example standards for healthcare.

Some countries have started to enforce the use of standards by making them mandatory for suppliers or by putting them on a national 'comply-or-explain' list. The same is true on the EU-level.

Tools

Tools should not be the main focus when implementing information security within your organisation. A lot can be done with simple office software such as spreadsheets and text processors. Only when numbers grow, especially the numbers of incidents, special tooling may be necessary:

- incident management: for example a trouble ticket system
- reporting: integrated tabular and graphics
- security management: risk management and compliance tooling

These tools are intended specifically for security management. Of course there are many more tools in use as part of implemented security measures.

References

ISO 27001, ISO 27002: *http://www.iso.org/iso/home/standards/management-standards/iso27001.htm*
PAS 555: *http://standardsforum.com/tag/pas-555/*
COBIT: *http://www.isaca.org/COBIT/Pages/default.aspx*
ISF: *https://www.securityforum.org/*

Further reading

Cyber security for boardroom members:
http://cybersecurityraad.nl/assets/1502517_VENJ_Cybersecurity_UK_vdef.pdf
Starterkit information security (Dutch):
https://www.surf.nl/binaries/content/assets/surf/nl/2010/SURFIbo+Starterkit+informatiebeveiliging+definitief.pdf
UCISA Information Security Management Toolkit: *http://www.ucisa.ac.uk/ismt*
Uninett: *https://www.uninett.no/en/tjenester/security-management-uninett-cert*
Website Géant SIG-ISM: *http://www.geant.org/Innovation/SIG_TF/Pages/SIG-ISM.aspx*

[2] Information Security Forum