SHS Web of Conferences **10**, 00007 (2014)
DOI: 10.1051/shsconf/20141000007


# Problems and solutions of information security management in Latvia

S. Deruma

BA School of Business and Finance, Latvia

**Abstract.** Cyberspace is a virtual environment. Today, it does not matter which device you use for connecting to the internet. You are just in there...

In Latvia there are different views on information security management models, managerial duties and responsibilities, professional skills and competence in the private sector and the public sector, as well as skills and competence in the European business environment.

The question is how to achieve good relationship, successful collaboration and a secure environment in cyberspace, how to provide the holistic approach and security intelligence, how to map out a new attitude?

Security cannot exist as a standalone function, it should be integrated in the associated processes continuously supervising and improving the security management programme based on predefined criteria. Adopting a holistic approach with regard to security has proven to be a critical contributing factor to effective security in organizations.

## Introduction

Over the last 50 years, the scope of information security has developed from mainframe systems to the bring-your-own-device (BYOD), including smart grids.

The Latvian government's strategy is to enhance capability of information security and, by doing so, to provide assurance on reliable and properly protected information.

In October, 2012, a European Cyber Security Month took place which continued to highlight the importance of cyber security issues. During the month, the following common themes, drivers and challenges were set up by the European Network and Information Security

Agency (ENISA) paid special attention to:

- Increased importance of ICT national coordination;
- Cooperation between the public and private sector;
- International cooperation;
- Reinforced incident response;
- Effective crime control;
- Critical infrastructure protection (Llinás, 2012).

This is the right place and the right time to continue discussions about cyberspace security, information security management and associated problems and solutions in Latvia.

## Research methodology and design

The objective of the research is to stress changes of paradigm in security management model, to support a competitive, balanced and prospective corporate development.

The task of the paper is to analyse the comprehensive information security management elements in the context of governance.

At this stage, the research includes the drivers for determination of due diligence that is the element of information security governance.

1. Self-assessments of strategic, operational and individual level to align security architecture with organizational goals using different management tools and techniques, such as gap analysis, risk management, determination of capability maturity level, professional skills inventory, competency analysis and compliance assessment.
2. External assessments – independent evidence based on audits and security tests.
3. Internal (cross-functional) assessments, information security performance measurement.

## Problems

From a technology perspective, there is little that separates classical information security from cyber security. Cyber security is about securing data and systems in the global environment. It is just a perspective that changes. By adopting this point of view, cyber security has become a global concern by definition. Due to the nature of the problem, advances in cyber security are most likely to be achieved through political cooperation (Llinás, 2012).

Cyber security is not just about copyright and personal data theft. It has also military aspects, for example, to prevent activities of organisations like Wikileaks[1].

The results of a survey indicate that 66% of the Latvian population use internet on a daily basis (Eurostat, 2011). Cyberspace is a virtual environment. Today, it does not matter which device you use for connecting to the Internet. You are just in there... In that virtual place you do day-to-day activities such as communicating, shopping, paying bills, searching information, reading news, making business, controlling, managing something and someone.

Development of democracy and social networks expanded virtual environment and turned it into an effective collaboration platform for municipality, government, politicians, as well as bad guys who do not respect national borders – terrorists, hackers, political players.

An impact on democratic processes left by active participation of the population is indisputable. It covers education possibilities and information exchange using internet tools, though the dark side of it should not be ignored, data thieves are professional criminals deliberately trying to steal information see Figure 1. – How motivation of criminals changes.

In Latvia, lessons have to be learned from bank authorization leaks and flows of personal data, however, learning from own mistakes are too expensive.

It is obvious that people expand their knowledge and increase their awareness of information security and cyberspace protection.

I would like to stress that all kinds of internet users – end users, developers, providers or supervisors regardless of their age, business area and confidence – should expand their knowledge.

On the one hand, there are a lot of opportunities and challenges; on the other hand, there are negative aspects of Cyberspace, for example, fragmentation of users – segregation of virtual groups, stratification and cyberware.

---

[1] WikiLeaks is a multi-jurisdictional public service designed to protect whistleblowers, journalists and activists who have sensitive materials to communicate to the public. Since July 2007, we have worked across the globe to obtain, publish and defend such materials, and, also, to fight in the legal and political spheres for the broader principles on which our work is based: the integrity of our common historical record and the rights of all peoples to create new history.

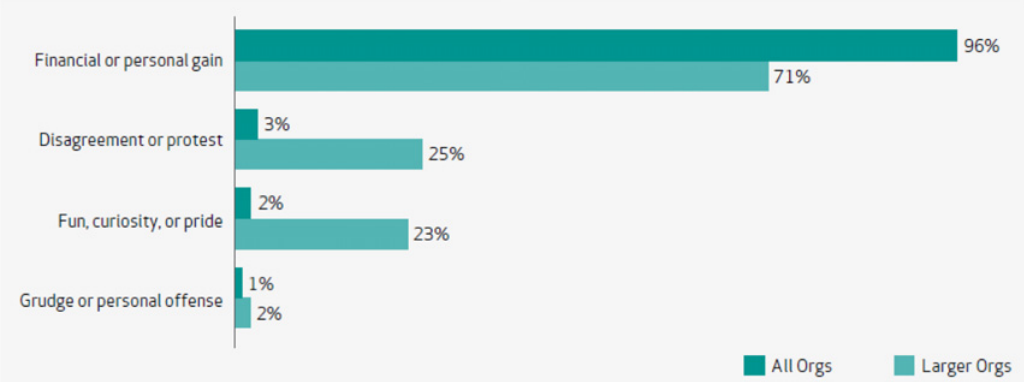


**Figure 1.** Changes of motivation of hackers, other criminals.
*source: Verizon, Data breach investigation report 2012.

**Figure 2.** The "noisy" security breaches published in Latvian media 2010 . . . 2012.

| | **Description** | **source** |
|---|---|---|
| 2010 | Data leaks from the State Revenue Service in electronic declaration system by Neo, the Fourth Awakening Nation Army (4ATA), and researcher of Latvian University. | Neo, Latvian University researcher |
| 2011 | Some problems with identification and authorization processes in information system of society counting. | Data State Inspectorate |
| 2012 | Internet bank identification and authorization problems | Master thesis: Security Analysis of Internet Bank Authentication Protocols and their Implementations |
| | The leakage of confidential e-mail data (Nils Usakovs Chairman of the Riga City Council) | www.kompromat.lv |
| | Deputy of the Saeima, Imants Paradnieks confirms that someone has published his internet surfing history | www.pietiek.com |
| | State Probation Service web application "holes" | Influent Ltd. audit report |
| | The special pop-up window containing Latvian police attributes and blocks the user's computers (Metropolitan police Virus). | Latvia Information Technologies Security Incidents Response Institution reports |

## Discussion

The crimes that involve computer networks and devices are as follows: spam, fraud, obscene or offensive content, cyber bulling, drug trafficking. They can be committed by means of hacking, inject viruses, malware (malicious code), denial-of-service attacks, identity theft, phishing or spoofing scams.

Just recall a scene from the movie *Live Free or Die Hard* (released as Die Hard 4.0) during which the main hero had to fight a gang of cyber terrorists who had hacked into the FBI computer system in order to take over control of the transportation grid, the stock market and remote control of the gas station to redirect the natural gas supply.

The same can happen in Latvia. How long can we live without electricity? Here is an example of an incident that took place in Riga in November, 2012.

Due to mistakes in the system, one day many street lights did not work in Riga. Emergency service operators of the local government agency "Riga Light" explained that computers were "frozen" and disconnected from the main system, therefore, many city lights could not be switched on (The National News Agency LETA, 2012).

In the view of all these conditions, it is a big challenge to create a national cyber security strategy (Draft Guidelines "Latvian Information Technology Security Strategy 2013–2018"), the whole strategy set up ranging from understanding a scope, identifying roles and responsibilities, projecting results and implementing appropriate performance controls.

## Comprehension – competence – collaboration

There are different views on information security specialists in regards with managerial duties and responsibilities, professional skills and competence in the private sector and the public sector, as well as skills and competence in the European business environment. The author of the paper would like to stress the importance of standardising the profession of information security manager, to define general and specific requirements for the profession and provide common understanding, regardless of a business area in which a company operates. It is important to understand consequences and disadvantages if requirements are not harmonized with international business environment.

The question is how to achieve good relationship, successful collaboration and a secure environment in cyberspace, how to provide the holistic approach and security intelligence, how to map out a new attitude.

One of the answers could be comprehension of the situation with cyberspace. "*To get stakeholder involve!*" said Neelie Kroes, Commissioner for Digital Agenda.

Such activities should be based on a good understanding by all stakeholders of the issues under their control that impact on the stability and resilience of the Internet; on the responsibility by all stakeholders to take appropriate actions, based on risk assessment, to prevent damages to the Internet and its users; and on an open and transparent approach to policy-making in the areas of concern to the stability and resilience of the Internet (ec.europa.eu, 2011).

Another one could be a shift in the historical approach from detective security management to preventive security management by providing understanding of what "security" looks like, establishing standards, creating policies that would lay the foundation of a unified concept for the industry development. Security cannot exist as a standalone function, it should be integrated in the associated processes continuously supervising and improving the security management programme based on predefined criteria. And do not forget about due diligence!

In finance, this term is used to describe a way of preventing unnecessary harm to either party involved in a transaction, an investigation or audit of a potential investment. Due diligence serves to confirm all material facts in regards to a sale.

In the field of Information Security, S. Harris offers the following definitions of due care and due diligence:

*Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees.* "And, [Due diligence are the]" *continual activities that make sure the protection mechanisms are continuously maintained and operational* (Harris, 2003).

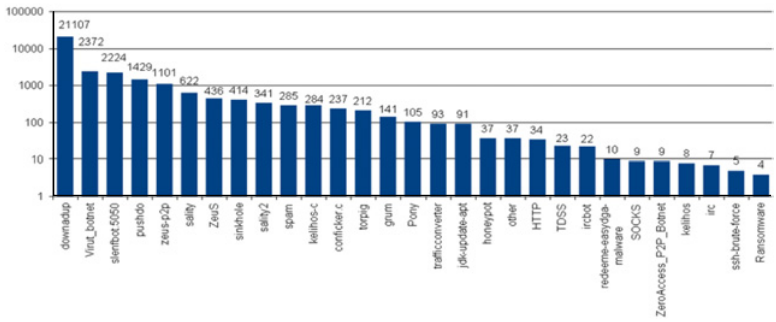


**Figure 3.** The security incident report of Cert.lv 2013 Q1.
*source: Latvian Information Technologies Security Incidents Response Institution.

Continual activities mean that people are acting to monitor and maintain the protection mechanisms, and these activities are on-going.

The latest pre-survey of Risk Management in Municipality Sector conducted by the author highlights trends and towards awareness of security risks. 30% of respondents consider that risk assessment does not take place at all; 50% of respondents do not have senior management support and consider that assessment is limited to formal meeting of requirements; 70% of respondents confirmed that they had experience in risk management.

If you want peace, prepare for war (Flavius Vegetius Renatus). Let us have a look at the Latvian cyberspace. Every month there are 1,000 high-priority security incidents and about 30 000 different harmful actions with Latvian IP addresses as shown in Figure 3.

The importance of protecting resources of an organisation and reasons behind it is showed by the following criteria: risk is a multiplication of *the value of assets, threat probability, and impact of vulnerability. In this case – i*f value of assets is zero, the risk is zero.

According to Risk management – Principles and guidelines, risk is defined in terms of the effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk is often characterized by reference to potential events and consequences or a combination of these. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence (AS/NZS 31000:2009).

Could you imagine what would happen if stakeholders did not know what resources have to be protected?

Code of Practice for Information Security Management recommends study of the following aspects during a risk assessment process:

- Information security policy,
- Organization structure of information security,
- Asset management,
- Human resources security,
- Physical and environmental security,
- Communications and operations management,
- Access control,
- Information systems (IS) acquisition,
- Development and maintenance of IS,
- Information security incident management,

- Business continuity management,
- Regulatory compliance (ISO/IEC 27002:2005).

All the aforementioned components are essential elements for maintaining information security governance.

## Conclusion

As long as data is collected, there will be people who will lose it, or be willing to break the law to obtain it (Jaquith, Down 2012) and once again I would like to stress the three words mentioned earlier – *comprehension – competence – collaboration*. Adopting such a holistic approach with regard to security has proven to be a critical contributing factor to effective security in organizations, information security management model implementation as a tool for ensuring effective governance as well as a factor to increase general competitiveness.

1. Information security management demonstrates understanding of the relationship between information security processes and broader business goals and objectives, business risks are reduced to an acceptable level and meet an organization's specific requirements.
2. Identify crucial issues of information protection and customize company's specific practices to support the governance of information and related technologies (e.g. establishes that relevant laws and regulations are being adhered to).
3. Demonstrate to enterprise customers their commitment to compliance, security and integrity and provide "Due diligence".

### References

[1] Down P. (2012). Monitor All Employee Activity Across PCs, Laptops & the Internet, SpectorSoft Corp., published at www.frontiertechnology.co.uk/wp-content/uploads/2012/10/SpectorSoft-Presentation-24-Oct-2012.pdf.

[2] Harris, S. (2003). All-in-one CISSP Certification Exam Guide (2nd Ed. ed.). Emeryville, California: McGraw-Hill/Osborne. ISBN 0-07-222966-7.

[3] Kroes N. (2012). European commissioner for digital agenda, speech video published at youtube.com http://www.youtube.com/watch?v=hnzrJyNWgDE.

[4] Llinás M. (2012). Moving Towards a European Cyber Security Strategy, European Network & Information Security Agency (ENISA), published at enisa.europa.eu.

[5] Seybert H. (2011). Internet use in households and by individuals in 2011, Eurostat, published at http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-11-066/EN/KS-SF-11-066-EN.PDF.

[6] Vegetius, (4-5th century). Epitome of military science. Google Books. Books.google.com. Vegetius has: Igitur qui desiderat pacem, praeparet bellum.

[7] AS/NZS (2009). AS/NZS 31000:2009 Risk management – Principles and guidelines. Australian and New Zealand risk management standard.

[8] ISO/IEC (2005). 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization and the International Electrotechnical Commission.

[9] LETA (2012). Rīga grimst tumsā datorsistēmu kļūdas dēļ [Due to mistakes in the system, Riga's many street lights did not work] Latvia: The National News Agency LETA published at http://nra.lv/latvija/riga/83842-riga-grimst-tumsa-datorsistemu-kludas-del.htm.

[10] Verizonbusiness (2012). Dat breach investigation report 2012. published at http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

[11] Anonymous (2013). CERT.LV reģistrētie zemas prioritātes incidenti no 01.01.2013. līdz 31.03.2013. [Security incident reports on 2013 Q1] Latvia: Information Technologies Security Incidents Response Institution published at https://cert.lv/resource/show/354.

[12] Anonymous (2011). European principles and guidelines for Internet resilience and stability. European Commission: published at http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf.

[13] Anonymous (2012). Pamatnostādņu projekts “Latvijas Informācijas tehnoloģijas drošības stratēģija 2013–2018” [Draft Guidelines “Latvian Information Technology Security Strategy 2013–2018”] Latvia: Ministry of Transport published at http://www.mk.gov.lv/lv/mk/tap/?pid=40267912.