

Press-release

Information Security Risk Management: How to Avoid Adverse Effects

Moscow, 28 July, 2010

Security incidents causing financial and reputational damage to entities become more frequent; and it compels organisations to revise the existing practices related to risk management and information security governance.

Experience of the global economic crisis demonstrated that effective company's security governance and risk management becomes substantially more critical in a challenging environment. The companies whose business largely depends on information systems operation have managed to overcome the crisis more successfully only if they managed to solve the issues of counteracting the adverse impact on their informational infrastructure (such as DDoS-attacks, unauthorized intrusion into a network for stealing or destroying information, etc.) along with general economic issues. Competent management of specific risks within the information environment such as process, technical, and project risks, as well as the risks related to implementation of new information systems and service applications is also very important.

Disregard of problems related to detecting and monitoring of information security risks results in substantial losses, both financial and image ones, for all companies, entities and organizations regardless of their size or field of activity. This can be exemplified by online shops and telecommunication service providers who fell victim to attacks on their information resources in recent years, as well as some financial corporations providing services all over the world.

This year, the Financial Industry Regulatory Authority (FINRA) reported serious violations of the corporate security policies at Lincoln Financial Group, one of the major U.S. holding companies, resulted in potential threat that the personal data of customers of a group of companies and individuals who applied for services, could be used by abusers.

As a result of an audit, it was revealed that the company personnel and its affiliates had common passwords assigned in 2002 for simplification of administrative functions with customer data. The passwords did not change for eight years and the access to information was provided to an excessive number of employees, including dismissed employees to whom the access was still available. The customer data could also be accessed by outsiders. Besides, the company made a number of technical mistakes which resulted in an open access to the customer data. Thus, the system generating mailouts to customers saved electronic copies of those letters in a customer correspondence file, thus enabling a customer or his/her agent to have access to a safe portal of the company and information of other customers, in particular, their addresses, dates of birth, contract numbers, value in accounts and transaction activities.

A few months ago, it was reported that logins and passwords of the company's authorized brokers and agents, intended for logging into the safe web-site that contained personal data of the individuals who applied for life insurance (addresses, Social Security Numbers and numbers of driving licenses, information of health and loans) were printed in a brochure intended for the use by brokers and agents only. The brochure was published openly on several agent web-sites. As a result of forensic examination and internal investigation performed by the company, no irrefutable evidence of unauthorized access to the customer data was found, neither of the abuse of the customer data. However, on July 20th this year, the company had to notify 26,840 individuals of the violations and to offer them free services as compensation. Besides, Lincoln Financial Group services had to notify 1.2 mln of its customers of violation of their personal data storage and risks related to possible potential threats.

Hendrik Ceulemans, a renowned expert, member of ISACA, author and presenter of dozens of workshops on IT and information security systems management for IT-management in the European Commission has thus commented the situation at the Financial Group: ‘Absence of adequate policies and/or practices for information security risk management and security governance resulted in three substantial incidents at an important financial company during the short period of time. In contravention of all existing rules, access passwords and lists of individuals having the relevant rights were not corrected for years, and confidential information was not properly protected, but it was published in publicly accessible sources. These incidents devastated the company’s’ image and revenues, and worse, destroyed its customers confidence.’

In order to avoid such mistakes, it is not enough to have a clear and correct idea of risk management and its application in the field of information security only but it is also required to apply one’s knowledge in a particular field of activity. The original courses of Hendrik Ceulemans at Informzaschita Training Center (<http://www.itsecurity.ru/>) organized at numerous requests from customers are aimed to guide organizations in preventing these disasters. The main objective of the Risk Management course, (http://www.itsecurity.ru/edu/kurs/kp_41.html) is the assimilation by professionals of the best world practices of risk management and acquisition of strong skills in practical application of evaluation and information security risk management techniques. The course focuses on methods for mitigating information related risks to acceptable level, selection and application of adequate controls including in the IT sphere. The author of the course has special focus on the comparison of risk management methodologies, commercial substantiation of their application within the IT, examples of controls, risk management, analysis of incidents and guidance for practical implementation.

Often, when evaluating the organisation’s cost structure, in a challenging economic environment, some managers blindly cut development investments or operational expenses. Actually, the most appropriate approach is to analyze the company’s functioning related to its information management and to align its IT-services with its real needs. This evaluation will enable to understand which enhancements are required in the area of information security and risk management. The program of the Information Security Governance course (http://www.itsecurity.ru/edu/kurs/kp_42.html) is aiming at informing information security managers on the analysis of risks and incidents, and implementation international best governance practices in a transparent management culture.

The courses are organized with cooperation of Informzaschita Training Center, (the leading Russian training center in the sphere of information security training, and InfoGovernance, a European company based in Belgium). The Risk Management course sessions will be held on 24–25 August, and the Information Security Governance – on 26–27 August. Training will be held in English with consecutive translation. Due to the limited number of participants, the organizers recommend to file requests for training expediently. Registration for participation in the course may be filled out here (http://www.itsecurity.ru/edu/zayavka/za_main.html).

Informzaschita Training Center

Informzaschita Training Center (<http://www.itsecurity.ru/>) is the leading specialized center in the sphere of training for information security (license No. 023947 of the Education Department of Moscow city, state accreditation certificate No. 0296), and it is a part of Informzaschita Group of Companies (<http://www.infosec.ru/group/>).

In the training center, professionals undergo training and upgrade their skills attending more than 70 training and integrated courses. Original author’s and authorized trainings are also held, as well as training of specialists for the work with products of such companies as Informzaschita, Crypto-pro, Kaspersky Laboratory, Aladdin, Application Security, Assuria, Clearswift, IBM (ISS products), Microsoft, Positive Technologies. Company certificates of training and state documents of skills

upgrade are issued. Since 1998, more than 25,000 professionals from 3,000 state organizations and business entities from 19 countries trained for information security in the Center.

Lincoln Financial Group

Lincoln Financial Group (marketing name of Lincoln National Corporation and its subsidiaries) was founded in 1905 and, today, it is one of the largest U.S. holding companies with headquarters in Philadelphia (USA). As at 31 March, 2010, the corporation manages assets for the amount of \$146 bln. Lincoln Financial Group provides diversified financial services, including life insurance, financial planning and many others.

Hendrik Ceulemans, CGEIT, CISA, MCA, MBA

InfoGovernance bvba

Telephone : +3215621019

Belgium

hendrik.ceulemans@infogovernance.com

www.infogovernance.com

Hendrik Ceulemans is the Principal of **InfoGovernance**, offering IT governance, information security governance and risk management consultancy and training services. Areas covered aim particularly to improve IT governance and information security governance using CobiT, Val IT and the ISO 27002.



Hendrik holds a CGEIT (Certified in Governance of Enterprise IT), a CISA (Certified Information Systems Auditor), a MCA (Master in Computer Auditing) and a MBA (Master in Business Administration).

Hendrik Ceulemans is a co-founder and served seven years as the President of the Belux Chapter of the Information Systems Audit and Control Association (ISACA).

Recent Experiences

Hendrik lectured seminars and workshops, and consulted on IT governance, risk management, information security governance and information audit in Canada, India, Morocco, Senegal, South Africa, Tunisia, the USA, as well as in twenty-two European countries.

Particular governance coaching and consultancy is going on for **Pension Fennia**, a pension insurance company in Helsinki. Hendrik coaches and assists the company's management with controls and risk self assessments in IT and the business entities, as well as with the implementation of a tailored governance improvement program.

At the **European Commission** (EC) Hendrik trained during the last eight years more than 300 IT, security and audit professionals in IT governance. Moreover, he trained some 150 professionals in information security and risk management. Furthermore, he assisted the EC on the implementation of risk management and CobiT. These activities have contributed in an important way to change the organisation culture in the direction chosen by the Commission.