PREFACE

IT Security: From products to process driven business continuity

Prof. Dr. Heinz Thielmann
Fraunhofer Institute for Secure Information Technology

The global information society is increasingly dependent on electronic networking and exchanging "electronic goods" with high economic value, both in private life and in business. Whereas private individuals are used to manage their own risks, managers of organizations are made responsible for managing the risk in such a way, that the organization will survive and will be able to continue their electronic business processes, even in case of internal or external attacks or in case of failure of networks, systems and components. IT Security is no longer an isolated issue of the IT manager, but requires attention on the top level of each organization. There is no difference between enterprises and public organizations, such as Governments and Healthcare. The view on IT Security moves from *product level* up to *solutions* and *process driven business continuity*. IT Security changes from a cost factor to an investment factor. New auditing and consulting methods are centered around "Return on Security Investment" (ROSI).

This preface provides a framework for international requirements on IT Security, driven by guidelines, legislation and research programs. Products and solutions from vendors of information and communication technologies should contribute to this framework and should support management to decide for appropriate solutions minimizing their risk and guarantee for their business continuity.

Security guidelines and legislation

Worldwide, the *OECD Guidelines on the Security of Information Systems and Networks* (Security Guidelines) propose the development of a "culture of security" to ensure the stable evolution of the digital economy and information society. The economic and social benefits have the potential to accrue on a global scale. In addition to the familiar concerns about the security of electronic commerce, hacking, privacy and cyber crime such as consumer fraud, there is the added vulnerability of society due to its dependence on information systems and the spectre of cyber terrorism. The main policy impacts from the OECD are:

- Raising awareness of the importance of the security of information systems and networks for safeguarding critical infrastructures, as well as business and consumer information.
- Highlighting and increasing knowledge of the Security Guidelines among all organizations who use information systems and networks.
- Providing guidance on the application of the Security Guidelines, using case studies of business, civil society and country experiences.
- Building awareness and, as appropriate, consensus on policy frameworks for the security of information systems.
- Exploring the use of technology and security standards in safeguarding information system infrastructures, as well as information stored in systems and on networks.
- Encouraging the development and promotion of security architectures for organisations that effectively protect information systems, as well as consumer and business products that include "embedded" security features to enhance their use of information systems.

Enterprises operating globally may be subject to several legislations and local companies may be subject to legislation from entirely different regions of the globe. Laws are overlapping, jurisdictions are becoming irrelevant, and corporate concern is growing. In the wake of prominent management failures, governments are under intense public pressure to pass more laws and regulations.

In the USA the Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley (GLB) and the Health Insurance Portability and Accountability Act (HIPAA) became law. In Europe and Japan the Data Protection Directives take aim at preventing identity theft and privacy violations. 21 CFR Part 11 in the USA and Annex 11 in Europe are written to regulate information pertaining to pharmaceutical R&D and manufacturing. BASEL II rating standards and certification according to ISO 17799 (BS 7799) meanwhile are on the top agenda for enterprise security.

Sarbanes-Oxley (SOX) and SAS 70: The SOX legislation is

aimed at making companies more transparent and eliminating risks to investors and the public at large. SOX is intended to reassure the public regarding the transparency of auditing procedures and the reliability of financial disclosure. At the core of this issue is financial data and the operations with which it is managed. SOX is intended to prevent either third parties or corrupt management from wiping out or falsifying financial documents. IT security aspects and audit ability are therefore crucial. Although the jurisdiction of SOX only extends to companies listed on the US exchanges, the impact of this legislation can be felt globally. International companies may do business in a variety of locales, but will face compliance in all foreign subsidiaries if they are listed on the US exchanges. Moreover, SOX is relevant in any situation where a public US company does business with another vendor, *no matter where that vendor is located*. Listed companies must now assure themselves that their vendors are SOX compliant or suffer some of the same consequences as if they themselves were in violation. The answer to some of these questions is hidden within the SAS 70 CPA accounting standard. Under this standard, CEOs and CFOs of publicly traded companies must take *personal responsibility* for the effectiveness of internal controls over financial reporting.

The following issues must be addressed by any organization seeking SOX or BASEL II or ISO 17799 compliance:

- Verification: Who is the originator of the data?
- Who is the recipient of the data?
- Are the sender and/or recipient authorized to send and receive?
- Transaction security: Are the data streams secure?
- Document security: Are the documents secured?
- Financial data security: Can the data be falsified? Is integrity assured?
- Monetary flow: Can funds be moved without proper authorization?
- Data storage security: Can documents be destroyed, ex-post changed or content be altered?
- Non-repudiation: Is the sent document legally effective and binding?
- Can the content and signature be relied upon?
- Last but not least, are the IT risks perpetually verified, evaluated and managed?

Management must identify the process based relationships most critical to the company, pinpoint existing internal and outsourcing organization gaps in process and controls that may increase risk and enhance existing activities with a more encompassing framework for internal controls.

BASEL II, which takes effect in January of 2007, is a revolution disguised as regulation. It is a mandatory international standard which must be implemented by all banks. Basel II's core set of regulations require banks to analyze their credit portfolio, not only through a traditional rating methodology (cash flow, liquidity, profitability, market risks, equity to debt ratio, etc.), but also through the identification and quantification of "operating risks." These risk evaluations must encompass a variety of departments including R&D, IT, manufacturing, and human resources. They must also take into account possible business interruptions due to strikes, disasters, organizational problems, and the ability of a corporation to manage these various crises. In order to extrapolate future risks, companies must keep and maintain operational data for at least 3 years. The accumulated effect of these rating changes across a bank's entire lending portfolio may very well necessitate an adjustment of the bank's capital reserves up or down. Basel II will therefore have a significant impact on the ability of banks to grant loans, the interest rates of those loans and *who they chose to grant those to.*

The primary driver for Basel II is the understanding that financial information alone is insufficient to assess a company's risk situation. Regulatory bodies and banks themselves now recognize that operational risks can change the overall risk rating by as much as 15% to 25%. Today's companies rely heavily on Information Technology (IT) to bear the brunt of managing a company's operation and processes. Operational risk assessment is therefore closely related to IT security.

Another aspect of risk assessment is the damage being done by systems failure. In December 2004 we saw a major failure of a US airline computer leading to a complete shutdown and the grounding of all flights. In August 2004, an employee of American Airlines entered an incorrect code that lead to a cascade of computer failures. The end result was a shut down, not only of AA's entire flight operations but also US Air. Why? Because US Air and AA both outsourced their IT operations and the breakdown affected the entire network. The danger is where one would least suspect it. Any high tech company invests large sums in R&D. Its easy to see how a disgruntled employee could send valuable technical know how to a competitor by means of a simple "mouse click" and earn more money in seconds then he can in years of salary. Patents can be passed on and revealed to competition. Imagine the risks pharmaceutical companies face. One could publish research and drug secrets prematurely, leading to a denial of a patent application, all because the technology was made available in the public domain.

It all leads to one conclusion: The IT systems at the core of today's operation must be secure in all respects. This is exactly what the BASEL II regulation seeks to ascertain: To what extent is the lender exposed to such risks and how does that fit into the ratings system?

A distinction must be made between systems security and software security. Systems security is related to the physical risks. Is the system protected against fire and water damage? Is there a back up system? Where is the back up system located? Is there a fail safe system? Is there a managed approach to safety? Is there a perpetual control system? Software security deals with software reliability and data integrity. Can one steal data? Can the data base be wiped out? Can files be altered? Can dates be changed? Is there an authorization procedure which is secure? Can identities be stolen? For example: In 2004, a US flight was forced to land prematurely because the authorities believed that one of the passengers was on a wanted list. However, after taking the individual and his luggage off the plane it was discovered that the person's identity had been stolen and the suspect was not a criminal, but a victim.

IT security is therefore a major topic within any discussion of Basel II. Risks inherent in IT operations can have significant repercussions to a company's credit rating. As with SOX, there is an upside to the story. An awareness of internal risks can only add to company's ability to cope with them. Moreover, SOX compliance and the "operating risks" of Basel II focus on many of the same questions. A solution to one problem, can deal effectively with the other.

Japanese Data Protection Directive: This legislation applies to private companies in Japan that handle personal or financial information such as payroll data. However, it excludes the media and writers. Under this regulation, companies must notify individuals that financial data has been acquired and specify the purpose for which any such data will be used. This directive will be followed by legislation for the health care, finance and telecom industries. Compliance must include the ability to safeguard personal data and protect it against loss, failure and disclosure.

Security Research: The European view

Security has been included in the list of priority research themes in the EU Commission proposal for the 7th Framework Programme for Research & Development (2007-2013). Security makes a timely entry into the list of research themes to be undertaken swiftly, in order to respond to highly societal demand in the face of new security challenges and to enhance the competitiveness of the Security Industry. Security Research forms part of the Security and Space thematic priority for cooperative research for which a common budget allocation of several hundred Mio € per year is proposed. Security in Europe is a precondition of prosperity and freedom. 'A Secure Europe in better World', adopted by the European Council, addresses the need for a comprehensive security strategy encompassing both civil and defence-related security measures. Security related research is an important building block in supporting the Common Foreign and Security Policy as well as for realising a high level of security within an EU-wide area of justice, freedom and security. It will also contribute to developing technologies and capabilities in support of other EU policies in areas such as transport, civil protection, energy and environment. Existing security related research activities in Europe suffer from the fragmentation of efforts, the lack of critical mass of scale and scope and the lack of connections and interoperability. Europe needs to improve the coherence of its efforts by developing efficient institutional arrangements and by instigating the various national and international actors to cooperate and coordinate in order to avoid duplication and to explore synergies wherever possible.

The activities set out below will complement and integrate the technology- and systems-oriented research relevant to security which is carried out in other themes. They will be mission-oriented, developing the technologies and capabilities as required by the specific security missions. They are by design flexible so as to accommodate as yet unknown future security threats and related policy needs that may arise, stimulating cross-fertilisation and the take-up of existing technologies for the civil security sector, European security research will also encourage the development of multi-purpose technologies in order to maximise the scope for their application. Activities are as follows:

- Protection against terrorism and crime: delivering technology solutions for threat awareness, detection, prevention, identification, protection neutralisation and containment of effects of terrorist attacks and organised crime.
- Security of infrastructures and utilities: analysing and securing existing and future public and private critical/networked infrastructure (e.g. in transport, energy, ICT), systems and services (including financial and administrative services).
- Border security: focusing on technologies and capabilities to enhance the effectiveness and efficiency of all systems, equipment, tools and processes required for improving the security of Europe's land and coastal borders, including border control and surveillance issues.
- Restoring security in case of crisis: focusing on technologies in support of diverse emergency management operations (such as civil protection, humanitarian and rescue tasks), and on issues such as interorganisational coordination and communication, distributed architectures and human factors.

The above four horizontal areas will be supported by the following themes of a more cross-cutting nature:

- Security Systems Integration and interoperability: focusing on technologies to enhance the interoperability of systems, equipment, services and processes, including law

enforcement information infrastructures, as well as on the reliability, organisational aspects, protection of confidentiality and integrity of information and traceability of all transactions and processing.

- Security and society: mission orientated research which will focus on socioeconomic analyses, scenario building and activities related to: the citizen's perception of security, ethics, protection of privacy and societal foresight.

Research will also address technologies that better safeguard privacy and liberties, and will address vulnerabilities and new threats, as well as the management and impact assessment of possible consequences. Inputs to meet the vision for Security Research will be provided by the European Security Research Advisory Board (ESRAB), forum where the users of security research i.e. the "demand pull" and the security suppliers i.e. the "technology push" meet to advise the Commission on security research needs.

International Regulations affecting IT Security Strategies & Policies

Sarbanes-Oxley (SOX)	U.S. Securities and Exchange Commission (SEC)	CobiT framework—Authentication, access controls, user account management, credential life cycle management, non-repudiation and audit controls	Companies publicly traded on U.S. exchanges	November 2004
Gramm-Leach-Bliley (GLB)	U.S. Office of the Comptroller of the Currency (OCC)	Authentication, access controls, encryption, data integrity controls and audit controls	All financial instructions regulated by the OCC	July 2001
IPAA Security	U.S. Department of Health and Human Services (DHHS)	Authentication, access controls, transmission security, audit controls and data integrity	Healthcare organisations in the U.S.	April 2005
21 CFR Part 11	U.S Food and Drug Administration	Authentication, access controls, data integrity controls, audit controls, encryption and digital signatures	Companies regulated by FDA (i.e. pharmaceuticals)	Final Guidance August 2003 (original deadline was 1997)
Annex 11 Computerized Systems	European Union (E.U.)	Access control, credential life cycle management, logging unauthorized attempts, recording identity of operators, and audit trails	All organizations producing medicinal products in the E.U.	Varies by country
European Data Protection Directive	European Union (E.U.)	Measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access	Companies conducting business in E.U. member nations	1997-2002 (varies by country)
Basel II	Basel Committee on Banking Supervision	FFIEC framework—Access rights administration, authentication, network access, operating system access, operating access, remote access, logging and data collection	Global financial service organizations including internationally active banks	2007
Japanese Data Protection Directive	Japanese Government	Safe-keep personal data against loss, system failure and leakage, i.e. unauthorized disclosures	Japanese private business	May 2005