Crying for the Moon?
Current Challenges in Corporate Information Security Management

Ulrike Hugl
Department of Accounting, Auditing and Taxation, University of Innsbruck, Innsbruck School of Management, Innsbruck, Austria

Keywords: Information Security, Intelligence Gathering, Cloud Computing, Big Data, Social Business, Hacking, Social Engineering, Economic Espionage, Industrial Espionage, Counter-measures.

Abstract: The ability to respond to the evolving challenges in corporate information security management is not a destination but rather a journey. To contest the race means to accept the dare, but being aware of the fact that offenders are normally one step ahead. Understanding threats and attackers' methods and strategies is a crucial issue towards protecting corporate assets. This work aims on presenting an overview of current information security-related trends, it explains possible internal and external motivated offenders and reveals related organisational weak spots. Moreover, it highlights some starting points for organisational prevention measures.

1 INTRODUCTION ON KNOWLEDGE, KNOW-HOW, RISKS AND DATA GATHERING

Information has become a crucial asset of all organisations. Especially the fast adaption of new information and communication technologies, mainly distributed throughout the Internet, as well as manifold software and tools – and, in addition to that, the 'human factor' (e.g. malicious insiders or whistleblowers) give constantly rise to the need for a critical reflection and up-to-date efforts on information security management.

The right *knowledge* at the right time is more topical than ever. Knowledge is power. Practical protection of corporate data (as information units), information (as base for knowledge) and derived *know-how* is a crucial resource of corporate success in times of keen competition. In addition, entrepreneurial acting is ongoing characterized by intentionally taking risks. In this sense, successful management always means to accept an intentionally calculated risk and to anticipate consequences of relation activities. Hence, the management has to make sure the organisation's future, existance and ability to act.

According to Wurzer (2011), the characteristic of *know-how risk* is freatured by the kind of damage. He distinguishes four categories of potential kinds: diffusion, destruction, substitution and imperfection. Diffusion means know-how loss based on unwanted, unintentionally and uncontrollable discharge of information to third parties (e.g. espionage, observation, stealing, disclosure of information, staff turnover); destruction is characterized by a loss of know-how based on a durable non-availability of know-how resulting from an active process of destruction (e.g. data loss, fire, sabotage); substitution relates to an accomplished leakage of availablity based on a contentual, temporal or organisational limitation (e.g. technological development, product lifecycle, competition changes, needs of customers), while imperfection is defined as loss of the active availability based an a contentual, temporal or organisational limitation (e.g. insufficient documentation, usage and organisation).

In general, attacks can arise from inside or from outside the organisation, whereby attack strategies may be legal or illegal. Potential interested parties are for example intelligence agencies to increase competitiveness of the economy in-country, competing companies, malicious insiders or whistleblowers (current and former employees with specific knowledge about crucial information and his/her organisation's (information) systems) or capital market agents and (organised) hackers.

Hugl U. (2013).
Crying for the Moon? - Current Challenges in Corporate Information Security Management.
In *Proceedings of the International Conference on Knowledge Discovery and Information Retrieval and the International Conference on Knowledge Management and Information Sharing*, pages 579-586
DOI: 10.5220/0004700605790586

An evaluation of different scenarios regarding legal and illegal sources of *data gathering* (meta data analysis, open sources intelligence, and various other data aggregated by intelligence agencies) illustrate a high degree of conformity regarding the offenders' objectives as well as a an enormous variety of analysis methods (Tsolkas and Wimmer, 2013). According to Wurzer (2011), such attacks can influence organisations' know-how in four categories in connection with the above-mentioned kinds of damage, namely diffusion, destruction, substitution and imperfection:

- *Objective Technical-bounded Knowledge* may entail potential risks in the range of construction plans, documentations, patent specifications, reports, software, copyrights, key technologies, industrial espionage, computer virus attacks, unintended loss, intended operating error, irregular documentation, incompatibility of infrastructure, missing up-to-dateness or usability of data pools, and others;
- *Personal-bounded Knowledge* with potential risks mainly related to 'the heads of employees', for example missing skills, demotivation and resignation of employees and/or consultants, staff transfer to other organisations, behaviour (legal or illegal) as well as recruiting;
- *Organisational-bounded Knowledge* with potential risks in the range of methods, design of production processes and routines, the organisational structure, internal and external cooperation, outsourcing, mergers & acquisitions and related external access to know-how pools, the constitution of teams, know-how transfer to other organisational units, and others;
- *Environmental-bounded Knowledge* with potential risks in the range of customers (e.g. change of preferences), suppliers (loss of buying sources), competitors (cross-sector cooperation, benchmarking results), technological development, etc.

As a consequence, organisations are forced to carefully reflect these mentioned knowledge pools and to increase awareness, especially with regard to questions like 'Who is -based on which sources- searching for my data and why?', 'Which data are being processed and used?', and 'What about an adequate data protection, based on internal as well as external cooperation?'.

The rest of the paper is organised as follows. The next section points out current challenges: first, present foci of the EU in the field of security technologies; second, information security-related trends like cloud and mobile computing, big data, social business, hacking and social engineering; and third, aspects of intelligence gathering to spy on organisations. The third section highlights some potential prevention measures for companies' information security management. The work closes with summarizing remarks.

2 CURRENT CHALLENGES

2.1 Foci of the European Union

At the global level, the European Commission aims on the creation of a so-called European knowledge society. The Security Programme in the EU and The Defense Advanced Research Projects Agency in the US fund security technology (R&D) highlighting the following typology of security technologies (EU, 2012):

- *Border, Aviation, Port, and Cargo Security* cover technologies for human identification and authentication, passenger and baggage screening, cargo screening and container tracking. Research in this area focuses on conventional biometric identifiers (fingerprints, iris scan, face recognition, voice analysis, hand geometry, palm vein, etc.), multiple and multimodal biometrics, behavioural biometrics, radio frequency identification (RFID) tags, smart cards micro-electronic mechanical systems (MEMS), surveillance and detection technologies, and more.
- *Biological, Radiological, and Chemical Agents Prevention* is an expanding area focusing on the detection of and protection from intentional attacks (from both state and non-state actors) and natural hazards (e.g. bird flu). Detection tools include a vast array of chemical, biological and radiation detectors, from conventional 'puffer devices' that detect trace amounts of explosives, to technologies such as neutron resonance fluorescence imaging, which can scan large volumes of cargo or luggage down to the atomic level. Protection tools include vaccines, protective clothing, blast absorbing materials, neutralizing agents, and decontamination materials.
- *Data Capture, Storage, Mining and Profiling* focuses on data handling at various levels, the semantic web, mesh networking and grid computing, devices for intercepting communications signals and related information flows, and more. So-called Intelligence Led

Policing (ILP) points towards a merging of law enforcement, counterterrorism, and disaster response technologies. Communication across disparate (and formerly totally independent) national and international agencies has become more and more important.

- *Emergency Preparedness and Response Technologies* include vaccine stockpiles, communications systems, control systems for situational awareness, decision support systems for real-time response, and data integration and fusion. Related technologies include Geospatial Web and Location-Based Services, comprising emerging systems of global epidemiological surveillance based on monitoring online communications and the World Wide Web.
- *Surveillance* is a special sector that can be either 'white' (visible and disclosed to the public) or 'black' (covert and invisible). A vast array of sensors across multiple modalities capable of collecting details that human beings cannot sense (infrared, ultrasound, subliminal images, electrical waves, and others) can be found in closed-circuit television (CCTV), microphones, stereo cameras, and more. Software to help identify suspicious behavior by detecting intruders, loiterers, or people moving against the flow of pedestrian traffic, and intention and emotion detection systems (for example smart corridors where people are subjected to an array of sensors capable of remotely detecting microfacial expressions, blood pressure, pulse rate, perspiration, and so on, and to process data in order to evaluate people's emotional arousal) are also under development.

While the second area more or less relates to the biological and chemistry sector, the other three categories refer to innovations from diverse engineering fields (for example computer science). To summarize: on the one hand, some of the mentioned innovations cover examples of (digital) security technologies potentially proposed to be use to fight against crime; on the other hand, they also may have great potential concerning new forms of attacks against organisations, especially in the field of economic crime and industrial espionage.

2.2 Information Security Trends

Currently, several major developments in the field of information security are exposing significant and growing gaps in information security programs may occur. The European Network and Information Security Agency (ENISA) highlights among others mobile computing, social technology, critical and trust infrastructures, cloud computing and big data as emerging threats. These and several other information security trends and vulnerability warnings are relevant for organisations and are presented in the following.

2.2.1 Cloud and Mobile Adaptions

At present, most organisations have developed some form of cloud computing and move more and more business processes, even regulated data and critical apps into the cloud. To speak with Hashizume et al., (2013): "Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

A German study in the field of cloud services as well as IT Service Management (ITSM) tools and processes presents the following results for organisations with more than 500 employees (IDC, Apr. 2013): Since 2012, about 75% of companies implemented cloud services and ITSM – thereby, its adequate management is the task of the IT department. What's the catch? Based on insufficient technical understanding (55%), speciality departments often implement cloud services without involvement of the IT department and without guarantee of an adequate services' management including all necessary security efforts. Based on the study's results, the latter seems to be a huge problem, especially in companies with more than 5,000 employees. Some further aspects: processes and services are changing very fast and require increasing maintenance (52%), the costs for such services are too high (48%), and the IT-environment is getting too complex to ensure a comprehensive ITSM (39%). – Summarizing, a moderate security management should focus on the integration into the existing IT-environment (early involvement of the IT department), on the monitoring of related service level agreements (SLAs) and on a clarification of responsibilities of the cloud provider (remarkable: only 14% of respondents estimate supplier and contract management as an important issue).

One emerging trend in cloud computing refers to an increase of PaaS (Platform-as-a-Service; e.g. NYSE Capital Markets Community Platform). PaaS provides a computer platform for developers of web applications which can be used only with minor

effort and without purchasing of related hard- and software. Such offerings also cover services for team collaboration and versioning, software as a service and others. By now, 82% of enterprises are using Software-as-a-Service, 51% Infrastructure-as-a-Service, and 40% Platform-as-a-Service (Skok, 2012). However, security remains the number one obstacle to adaption: in 2012, only 29% of companies (covering 128 countries) have implemented a cloud security strategy (PwC, Oct. 2012). Main concerns of information security professionals (worldwide) span from exposure of confidential or sensitive information to unauthorized systems or personnel (85%), over confidential or sensitiv data loss (85%), week system or application access control (68%), suscepibility to cyber attacks (67%), disruption in the continuous operation of the data center (65%), inablility to support complicance audits (55%), right up to inability to support forensic investigations (47%) (Frost and Sullivan, 2011).

Another crucial security-related issue refers to *mobile computing and applications*. For mobile devices like smartphones and tablets, many organisations also are asked how to best mix personal and corporate information. Anyway, the dominant endpoint is not a desktop computer, but a mobile device. Hence, organisations have to rise to this challenge regarding a secure and reliable availability of organisational data. Results of a study conducted by Frost and Sullivan (2011), covering feedback of 10,413 information security professionals from organisations around the globe, show that "[m]obile devices were the second highest security concern for the organization, despite an overwhelming number of professionals having policies and tools in place to defend against mobile threats" (first ranked are application vulnerabilities). And: Mobile device security products in place mainly are encryption (71%), network access control (59%), and mobile VPN (52%).

Mobile and *Bring Your Own Device (BYOD)* enables employees to work anytime and anywhere and to handle most business data and activities. This fact "[…] makes mobile devices a prime target for hackers and provides new entry points for attack. Also mobile devices are easily lost or stolen" (Deloitte, 2013). More specifically: 74% of respondents highlight vulnerabilities regarding an increased usage of mobile devices. The survey solely covers organisations around the globe working in technology, media and telecommunications (TMT) industries. Nevertheless, from those organisations with more than 10,000 employees only 64% provide specific policies for mobile devices and BYOD. Looking at the total survey pool (large and small organisations), 52% have such policies, but around 10% do not address BYOD risks at all. One of the biggest barriers to improving information security continues to be lack of budget (49% of respondents). (Deloitte, 2013) Sandboxing technology as a further trend tries to keep corporate data confined. Thereby, the user is only able to access information without its respective storage area.

In Germany, more than the half of employees are working partially mobile. 40% of companies have a mobility strategy, one quarter plan to implement one during the next six or twelf months. For 56% of IT decision makers IT security is the main trigger for mobile device management. Self-controlled registration of all systems or end devices in the nework (32%), remote access to devices (30%), as well as the technical separation of private and corporate applications (29%) are increasingly used functions. (IDC, Sep. 2012)

ENISA (Sep. 2012) reports manifold increasing threat trends in the field of mobile computing and mobile systems, most of all cross-platform threats, drive-by-exploits (unintended download of malware), worms and troyans, exploit kits (malicous programs), physical theft, loss and damage of mobile devices, data breaches of sensitive data stored on devices or being on the move over communication channels, phisihing, identity theft, and botnets (through infections of mobile platforms). In general, most notably cross-platform threats, hacking of mobile devices, attacks when using mobile platforms (e.g. for financial transactions), weaknesses from weak introduction of BYOD policies and related attacks of mobile devices and services, as well as the need for advancements in app security to improve mobile security can be highlighted. Despite all mentioned attack potentials, not more than 44% of companies (in 128 countries) have a mobile security strategy (PwC, Oct. 2012).

2.2.2 Big Data, Social Business, Hacktivism and Social Engineering

Big data is underway. More and more companies begin related projects to promote their market position and business intelligence and analytics (see e.g. Chen et al., 2012), for example regarding tailored customer services, the global supply-chain and better business information. Big data is "[…] a capacity to search, aggregate, and cross-reference large data sets" (Boyd and Crawford, 2012) and is "[…] used to describe data sets so large and complex

that they become awkward to work with using standard statistical software" (Snijders et al., 2012). On the one hand, big data can be applied to analyse malicious activities (based on data of employees' behaviour), it plays a crucial role in changing the organisation's information security approach to be more effective, and can for some reasons be seen as one of the highest priorities for companies. On the other hand, the relative newness of the area leads to a number of security risks. One crucial risk: big data evokes new methods to perform attacks. Hence, companies recognize the value of big data for security, but "[t]hey also must get in on the ground floor of any new big data projects that the business takes on, in order to understand the risks and develop strategies to manage them" (EMC, 2012).

Also *social media* will continue to transform information systems. There exist innovative opportunities to reach customers and to create positive branding. The negative side for companies are related security risks with regard to manifold opportunities for malware distribution, misinformation and misuse (especially in connection with BYOD). In addition, employees also may distribute (confidential) corporate-relevant information on online social network or other social media sites without being aware of issues like industrial espionage (e.g. carried out by competitors), economic espionage (carried out by intelligence agencies), potential starting points for social engineering techniques (so-called targeted attacks), and others. Based on sophisticated analysis methods on social media, for example, social network analysis (SNA) focuses on networks of relationships (groups of persons and organisations). Specific SNA-techniques are correspondence analysis, hierarchical analysis, social network analysis flow mapping, flow model data (analysis of social relationships) and multidimensional scaling (MDS). All these instruments unlock potential for attacks in diverse fields. Hence, "[a]s organizations increase their use of social media to capture the business benefits, they must also put in place strategies to manage the risks" (EMC, 2012). Nevertheless, in 2012, only 38% of companies from around the globe had implemented a related strategy (PwC, Oct. 2012).

Another growing security threats is *hacktivism* – the use of hacking techniques to promote political, social, ideological or religious activism (e.g. Anonymous via Distributed Denial of Service (DDoS) attacks). Throughout 2012, *hacking attacks* continued unabated. A study of Frost & Sullivan (Feb. 2013), covering opinions of about 12,400 information security professionals, comes to the following results: 56% are concerned about hackers (an attacker or group of attackers who seek and exploit weaknesses in a computer system or network), and 43% about hacktivists (whereby concerns are mainly remarked by respondents working in the insurance, banking and finance sector). Harry Sverdlove, chief technology officer of a security software vendor, states: "Hacktivists respresent the unpredictable factor, […] All it takes is a few individuals with an agenda or an ax to grind, and they now have the tools to launch distributed denial-of-service attacks or attacks to wipe out data. It makes for a much more dangerous combination." (Schwartz, Dec. 27, 2012). Furthermore, DDoS attacks, so-called Armageddon-style (high-bandwidth cloud) attacks, could overwhelm not just targeted websites, but also any intervening service providers (Schwartz, Dec. 27, 2012); (Schwartz, Nov. 27, 2012).

Hacker groups like LulzSec, hacktivist groups like Anonymous, and cyber criminals currently also use SQL injection as common attack vector against web applications. Hacktivism, extortion and vandalism are the main DDoS attack motivations, and publicly available hack tools on the World Wide Web enable attackers to spot users as well as passwords and to intercept Wi-Fi traffic (e.g. DroidSheep, Faceniff) (ENISA, Sep. 2012). Another trend in hacktivism seems to cover destructive attacks on critical infrastructure systems.

A further attractive entry-point for attackers is *social engineering* (see e.g. Applegate, 2009). Such attacks aim on an exploitation of a human's cognitive biases and psychological triggers. Examples are pretexting (creation and usage of invented scenarios), baiting (e.g. via leaving malware-infected physical media like a CD-ROM or an USB flash drive in an office), phishing for identity information, tailgating for access (e.g. an attacker walks in a corporate facility behind another person having an entrance key, RFID-tag, etc.), or getting the target to take certain action (e.g. disclosure of password access to a company's systems). Social engineering normally is combined with other forms of attacks and typically victims are oblivious of the attack.

2.2.3 Intelligence Gathering and further Opportunities to Spy on Companies

Information is the ‚new gold' in the 21st century. Current spheres of activitiy in the field of *information gathering* and with potential to harm

companies in different ways are for example Electronic Warfare (covering any action involving the use of and getting access to the electromagnetic spectrum and to control it), Signals Intelligence (SIGINT), Open Source Intelligence (OSINT), data mining processes, Communications Intelligence (COMINT), Electronic Intelligence (ELINT), Electronic Attack (EA), Electronic Countermeasures (ECM), (the above mentioned) social network analysis as well as social engineering, Competitive Business Intelligence (CBI), Open Source Intelligence (OSINT), (micro-)drones or unmanned aerial vehicles (UAV), and Human Intelligence (HUMINT) as intelligence gathering by means of interpersonal contact respectively information collected and provided by human sources, etc. Others are white collar crime, economic espionage and industrial espionage. Generally spoken, the latter aspects comprise (semi-)governmental organisations or individuals aiming on information gathering from different types of 'competitors', typically using a mix of all above quoted instruments. Several instruments are mainly used in the military sector, but also are relevant for all kinds of organisations. Anyway, *actors in the field of intelligence gathering* are intelligence service providers, capital market agents, intelligence agencies as well as competing companies (e.g. efforts regarding market and customer data, strategies, technologies, construction plans, R&D results etc.).

Another critical aspect leads to potential impacts for companies based on the *European Data Retention Directive* (EU, 15 March, 2006), implemented by law in most EU states. What about possible spy szenarios? First, mobility patterns: González, Hidalgo and Barabási (2009) analysed human mobility and derived patterns of humans' movements. Movement data generate data of humans and the economic cycle (see e.g. related products on market of the MIT-spinoff Sense Networks). Based on his data from the German Telekom (2009-2010), the politician Malte Spitz published his comprehensive movement and communication profile (including interacttive graphics, travelling and social network/relationship analysis) to warn against data retention (Biermann, Feb. 24, 2011). The results are more than profound. What does this probably mean to organisations and their employees? Movement data (e.g. based on mobile phone location) allow to segment groups regarding profession, social status, personal circumstances, relationship analysis, habits, routines, state of health, and others. Second, a combination of these issues regarding working *and* private life of employees may generate much more additional information. Third, according to Tsolkas and Wimmer (2013) some further relevant aspects can be pointed out: (1) Based on an analysis of all employees' mobile phones for a longer time, an exposure of communications chains, triggered by a specific event could be disclosed (e.g. similar patterns regarding the acquisition of a huge order). It is thinkable that, for example, such events occur more than once. In such cases, based on generated data, probably the arrival of a new event may automatically be predicted and deployed by an offender. (2) On the basis of social structures and networks of employees, it can be possible to identify the role of a specific person inside a group. If it is possible to identify functionally important persons of the organisation, diverse threat analyses are possible: poaching or interference of the person (e.g. during temporal limited and huge projects), attacking the person due to his/her habits or preferences, targeted approaching and sounding out of information (e.g. as preparation for eavesdropping). (3) Based on employees' location data of their smartphones using the same cell, most likely offenders are able to discover who is with whom at what location (restaurant, supplier, headquarters, etc.), also probably the purpose of a meeting. An example: if such a meeting is held at the headquarters of a competitor, an offender may draw conclusions from that (e.g. regarding a potential company take-over or negotiations about an intensive cooperation in a specific field, etc.).

Since PRISM, Tempora, XKeyscore and other disclosures of Edward Snowden, *Whistleblowing* is on everyone's lips. Currently in media discussed occurrences of spying in huge dimensions has brought the topic of extensive surveillance of governments to the public at large. However, the whole issue is not that surprising: huge surveillance activities of intelligence agencies in current times of technological opportunities as well as committed cooperation between such institutions are nothing new, notably not since ECHELON[i] and other communication surveillance equipment as well as relevant legislation after 9/11. Or as Weiße (2011) argues: Bringing the current situation to mind by asking 'what was?', and then questioning 'what is?' seems easy to be answered. We can multiply 'what was?' by the factor 10 and probably are at the 'what is?'. Currently, the European Union funds the project INDECT (intelligent information system supporting observation, searching and detection for security of citizens in urban environment;

http://www.indect-project.eu/). INDECT aims on the development of advanced and innovative algorithms for human decision making support in combating terrorism and other criminal activities, such as human trafficking, detection of dangerous situations and the use of dangerous objects in public spaces. Based on its tools and instruments (drones, CCTVs and computer-based analysis of related video data, face recognition, etc.), INDECT wants to support preventive work of police, Homeland Security Services and communities by pooling and combining these tools and instruments on related databases. However, opponents of the project assume the worst, notably much more surveillance in the public space. Related to companies, via INDECT developed instruments do have also huge potential for further activities in the field of information and intelligence gathering of attackers in the field of industrial and economic espionage.

3 COUNTER-MEASURES

Recurrent evaluations of the corporate initial situation may be a first step: Why are we on the market? What's the difference to our competitors? What are our most successful products or services? How do we assure sustained success? (Tsolkas and Wimmer, 2013).

In information security, humans are a very crucial factor (see e.g. Deloitte, 2013). Hence, people are part of the problem. Based on area- and department-specific guidelines, employees should know how to behave in specific situations. For examples: About what I am allowed to speak with third parties? What I am allowed to hand over?

The next step may be an analysis of the specific protection requirements on different protection levels, preferably together with the risk management, controlling, accounting and/or compliance department and possibly based on a scoring system. The related analysis determines specific protection levels for objects, processes and (in special circumstances) for staff (physically and key know-how-related protection), in addition for concrete danger, risks and potential harm. Furthermore, training and awareness may help to manage risks from diverse forms of attacks. Some examples for related topics are: understanding of security guidelines, strengthening of technological skills, knowledge of potential offenders' objectives in the field of economic and industrial espionage, dos, don'ts and responsibilities in cases of crisis management, forensic analysis (e.g. in anti-fraud management) as well as social engineering, hacking, and other attack strategies.

Further protection measures comprise the implementation of standardized security concepts like DIN ISO 27001 or COBIT (Control Objectives for Information and Related Technology). But: based on several involved persons (e.g. external auditors, employees etc.) as well as the servicing institution itself, one disadvantage may be that such standardization potentially can lead to new attack opportunities, for instance in the fields of social engineering, blackmailing, intimidation, or intended malicious acts of humans. The same can apply for consulting or other service providers.

What others can be done? One point is the development of attack-relevant strategies, for example an information security, a cloud, social media, and mobile device security strategy as well as one for employees' usage of personal devices on the company (see e.g. PwC, Oct. 2012). A further lever to protect corporate assets can be the implementation of whistleblower structures, help desks, hotlines, and the consideration of prevention measures 'fitting' with the organization's incentive and compensation systems. Furthermore, especially bigger companies afford the expense of a specific counter-espionage department (e.g. German Telekom).

4 CONCLUSIONS

The ENISA report results show that "[d]ata breaches are usually realized through some form of hacking, incorporated malware, physical attacks, social engineering attacks and misuse of privileges". Thereby, the main causal agents are negligent or malicious insiders and external attacks like hackers, hacktivists and other (cyber) criminals. (ENISA, Sep. 2012).

In this paper, on the one hand, several general challenges and trends with impact on an adequate and up-to-date corporate information security management were highlighted – on the other hand, some organisational prevention measures were presented. To summarize: Today's information security management is a fast evolving game of advanced strategies and skills. Former security models no longer seem to be effective. As starting points for an organisation's protection of organisational know-how and assets, both, the variety of external as well as internal offenders as well as current trends of attack strategies have to be continuously considered. Or to speak with Sun Tzu, a Chinese military general, strategist and

philosopher: "If you know your enemies and know yourself, you will not be imperiled in a hundred battles […] if you do not know your enemies nor yourself, you will be imperiled in every single battle."

REFERENCES

Applegate, S. D. 2009. Social Engineering: Hacking The Wetware! *Information Security Journal: A Global Perspective*, 18**,** 40-46.

Biermann, K. Feb. 24, 2011. Was Vorratsdaten Über Uns Verraten. *Hamburg: Die Zeit Online*.

Boyd, D. & Crawford, K. 2012. Critical Questions For Big Data. *Information, Communication & Society*, 15**,** 662-679.

Chen, H., Chiang, R. H. L. & Storey, V. C. 2012. Business Intelligence And Analytics: From Big Data To Big Impact. *Mis Quarterly*, 36**,** 1165-1188.

Deloitte 2013. Blurring The Lines. 2013 Tmt Global Security Study. New York: *Deloitte Touche Tohmatsu Limited*.

Emc 2012. Sbic Special Report: Information Security Shake-Up: Disruptive Innovations To Test Security's Mettle In 2013. Hopkinton (Ma): Security For Business Innovation Council (Sbic)/Emc (Rsa).

Enisa Sep. 2012. Enisa Threat Landscape. In: Marinos, L. & Sfakianakis, A. (Eds.). Heraklion: European Network And Information Security Agency (Enisa).

Eu 15 March 2006. Directive 2006/24/Ec Of The European Parliament And Of The Council Of 15 March 2006 On The Retention Of Data Generated Or Processed In Connection With The Provision Of Publicly Available Electronic Communications Services Or Of Public Communications Networks And Amending Directive 2002/58/Ec.

Eu 2012. Ethical And Regulatory Challenges To Science And Research. Policy At The Global Level. Luxembourg: European Union.

Gonzalez, M. C., Hidalgo, C. A. & Barabasi, A.-L. 2009. Understanding Individual Human Mobility Patterns. *Nature,* 458**,** 238-238.

Hashizume, K., Rosado, D. G., Fernández-Medina, E. & Fernandez, E. B. 2013. An Analysis Of Security Issues For Cloud Computing. *Journal Of Internet Services And Applications,* 4**,** 1-13.

Idc Apr. 2013. Idc-Studie: Deutsche Unternehmen Verlassen Sich Auf It Service Management Für Die Cloud. Frankfurt: *IDC Central Europe*.

Idc Sep. 2012. IDC-Studie Managing Mobile Enterprises In Deutschland 2012: Byod Hat Zenit Erreicht. Frankfurt: Idc Central Europe.

Pwc Oct. 2012. Changing The Game. Key Findings From The Global State Of Information Security®. Survey 2013. New York City: *Pricewaterhousecoopers LLP*.

Schwartz, M. J. Dec. 27, 2012. 7 Top Information Security Trends For 2013. *Informationweek.*

Schwartz, M. J. Nov. 27, 2012. Bank Ddos Strikes Could Presage Armageddon Attacks. *Informationweek.*

Skok, M. J. 2012. 2012 Future Of Cloud Computing - *2nd Annual Survey Results.*

Snijders, C., Matzat, U. & Reips, U.-D. 2012. "Big Data": Big Gaps Of Knowledge In The Field Of Internet Science. *International Journal Of Internet Science,* 7**,** 1-5.

Sullivan, F. 2011. The 2011 (Isc)2 Global Information Security Workforce Study. Mountain View (Ca).

Sullivan, F. Feb. 2013. The 2013 (Isc) Global Information Security Workforce Study. Mountain View (Ca).

Tsolkas, A. & Wimmer, F. 2013. Wirtschaftsspionage Und Intelligence Gathering. Neue Trends Der Wirtschaftlichen Vorteilsbeschaffung*,* Wiesbaden, Springer.

Weiße, G. 2011. Totale Überwachung. Staats, Wirtschaft Und Geheimdienste Im Informationskrieg Des 21. Jahrhunderts*,* Graz, Ares.

Wurzer, A. J. 2011. 1. Know-How-Risiken - Definition Und Systematik. In: Wurzer, A. J. & Kaiser, L. (Eds.) *Handbuch Internationaler Know-How-Schutz.* Köln: Bundesanzeiger.

[i]ECHELON is based on the UKUSA Agreement (1946) of intelligence agencies of the USA, Great Britain, Canada, Australia, New Zealand and others (so-called Third Parties). In 2004, concerns regarding economic espionage of European companies resulted in the closing-down of the facility in Bad Aibling (Germany).