Computer and Information Science; Vol. 5, No. 5; 2012
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Incorporating Information Security in Analysis of Business Strategy: A Conceptual Framework

Mingtao Shi[1]

[1] FOM Fachhochschule für Oekonomie & Management, University of Applied Science, Berlin, Germany

Correspondence: Mingtao Shi, FOM Fachhochschule für Oekonomie & Management, University of Applied Science, Bismarckstr 107, Berlin 10625, Germany. Tel: 49-171-288-1169. E-mail: Consulting_Shi@yahoo.de

Received: June 5, 2012 Accepted: June 27, 2012 Online Published: July 2, 2012

doi:10.5539/cis.v5n5p1 URL: http://dx.doi.org/10.5539/cis.v5n5p1

Abstract

The rise of Information Technology over the past decades has contributed to the increase of digital and electronic information processing greatly. As a result, information security has become a major strategic concern of firms and business strategy needs to incorporate information security deliberately. This study explores strategic implications of information security by conducting an empirical firm case study, an assessment of a national market and a more general industry analysis. The investigation is based upon concepts widely acknowledged in strategic management. The results argue the unambiguous necessity of incorporation of information security in the analysis of business strategy and suggest a number of strategic issues related to firm resources, market conditions and industry circumstances that are of essential meaning for strategy development. Some of these issues include privacy and anonymity, laws and regulations, natural risks and business continuity, informational assets and related knowledge, routines, software and hardware, trust and confident in e-markets, reputational advantage and buyer's loyalty. A conceptual framework is established to synthesise the results of the investigation.

Keywords: business strategy, information security, data protection, resource-based view, SPENT, five forces

1. Introduction

Broadly speaking, *technology* encompasses hardware, software, human-ware and organisation-ware involved in all kinds of products and processes within a firm (Hagström & Chandler, 1998). The concept of the value chain views the technology development as a supporting unit of a firm's primary activities (Porter, 1985). Obviously, the importance of technology in general has long been recognised in academia.

What practitioners have been observing since two to three decades is that *Information Technology* (henceforth *IT*) in particular has evolved to a distinctly vital technology. Businesses operating in a wide range of industries have become increasingly dependent upon the smooth performance and seamless operational integration of IT, which also provides infrastructural assistance for R&D, product and process design.

Under such circumstances, significant security issues arise, as firms utilise IT to acquire, access and process productive information, such as data related to research and production, and personal data, such as employee salaries and private addresses. *Information security* has become a major concern of business firms and matters strategically to their long-term competitive advantage.

This study aims at initiating a debate that focuses on the implication of information security during the formulation of *business strategy*, by discussing why strategic management increasingly requires managers to incorporate information security and what may be considered thereby. The remainder of the study first gives an overview of the management of business strategy before it turns to mention some terms frequently used in the field of information security. Strategic implications of information security are then analysed through case studies delineating specific issues of information security in a business firm and in a national marketplace. A brief and more general analysis based upon a strategy framework is added to the preceding case studies, examining the information security at the industry level. This paper subsequently suggests a conceptual framework aimed at enabling strategic planning to incorporate the essentials of information security effectively. Finally, some instruments for implementing security strategies are introduced and conclusions are drawn.

2. Business Strategy

Mintzberg, Ahlstrand and Lampel (1998) observed and identified ten patterns of strategy formulation. Although their study is an extensive exploration of the strategy theory, the contemporary business strategy has been significantly shaped by two major schools of thought, the *market-based and resource-based strategic management* (e.g. Makhija, 2003).

The market-based approach is rooted in the theory of industrial organisation postulated by Mason (1949) and Bain (1959). Extracting the knowledge from this field, Porter (1980; 1985) advanced the famed *five forces model* to allow the analysis of a firm's industrial environment, based upon which generic strategy can be derived. Besanko, Dranove and Shanley (1999) advocated that strategic analysis needs to also include factors in the broader market environment. The market-based thinking recognises that factors in the external environment, encompassing the *market and the industry*, determine the profitability of a business. Consequently, the firm must strategize to gain and hold a favourable position somewhere in its operational environment.

Strategic positioning is however only one side of the coin. Debates in the field of business strategy in the last three decades have increasingly focused on the internal sources of a firm to achieve Sustained Competitive Advantage (SCA). The resource-based view contends that firms perform differently in similar external environment because of their different skill sets underlying the products and services that firms deliver. Strategic resources, capabilities, competencies are the ultimate sources of SCA and positive firm performance is generated predominantly by evolutionary processes internal to the firm, involving *creation, development, improvement, accumulation, combination, and protection of the intangible and tangible assets of the firms*(Wernerfelt, 1984; Barney, 1986; Dierickx & Cool, 1989; Prahalad & Hamel, 1990; Barney, 1991; Conner, 1991; Stalk, Evans, & Shulman, 1992; Peteraf, 1993; Rumelt, Schendel, & Teece, 1994; Sanchez & Heene, 1997; Freiling, 2001; Barney, 2002; Peteraf & Bergen, 2003; Acedo, Barroso, & Galan, 2006).

3. Information Security

From the perspective of a business firm, *security* is not only a state that is free from risk, but also a process which continuously defines, contributes to the arrival at and preserves the state of minimal hazard. *Information security* consequently is about the risk avoidance of informational assets controlled or related to a firm. Notably, informational assets have increasingly become *electronic* and *digital*. A number of danger sources may negatively influence the safety of electronic information, such as organisational weaknesses, unintentional human errors, malicious human behaviour, technical failure and act of nature beyond control. The main task of information security is to understand the nature of these different types of danger, based upon which managerial and technical methods can be developed to encounter the risks.

It is widely recognised in the literature that information security is achieved from four major vantage points (e.g. Brenner et al., 2011; Eckert, 2009):

1) *confidentiality*: access to informational assets only through authorised persons;

2) *availability*: availability of informational assets whenever and wherever they are needed;

3) *integrity*: no unauthorised change of informational assets;

4) *compliance*: lawful and regulatory compliance regarding informational assets by firms and organisations.

Information security is not just about technical considerations, such as establishing a secure and reliable data connection between two dispersed operational units. Main areas of concern in a firm may for example include the *security of software, hardware, personnel and physical configurations; the control mechanisms for entrance, admission and access processes;* firm policies for *documentation, change and audit management;* treatment of *personnel- and business-specific data; business continuity management*. Nota benne, personnel and privacy data is a part of informational assets that must be protected, especially in terms of confidentiality.

The strategic importance of information security is analysed at three layers in the following sections. First, information and knowledge gained during an empirical firm study shall be presented to take a close look at the resource-based issues within a firm. Next, the SPENT model is applied to scan the market environment and to identify strategic issues in a national market. Third, the five forces model is employed to generate insights that may be observed in a wide range of industries. The investigation is conducted from the perspective of information security.

4. Resource-Based Implications: A Firm Case Study

This section first looks at the cornerstones of the resource-based strategic thinking, before the background of the case study is described. The methodology of the *qualitative research* is then delineated and elicited *empirical data* are presented, drawn upon which some strategic implications regarding information security are extracted in a discussion.

4.1 Resource-Based Strategic Thinking

Barney (1991) advanced four preconditions shaping firm resources to be strategic. First, resources must have *value*, enabling a firm to conceive of or implement strategies that improve its performance. Second, the value-creating resources must be *rare* and are not simultaneously possessed by many other firms. Third, resources are *imperfectly imitable* for one or a combination of three reasons: a) the ability of a firm to obtain a resource is dependent upon unique historical conditions; b) the linkage between the resources possessed by a firm and a firm's sustained competitive advantage is causally ambiguous; c) the resource generating a firm's advantage is socially complex. Fourth, there must be no strategically equivalent resource *substitutes* that are themselves either not rare or imitable. Dierickx and Cool's (1989) argued analytically similarly that strategic resources are time-consuming and costly to replicate (time compression diseconomies); strategic resources are reinforced to the extent that adding increments to an existing asset stock is facilitated by possessing high levels of that stock (asset mass efficiencies); accumulation of strategic resources is not only depend upon the level of concerned resource stock itself but also upon the level of other related stocks (interconnectedness of asset stocks); strategic assets need to be maintained constantly before they erode (asset erosion) and the resource accumulation process is rather random and unpredictable than deterministic in many cases (causal ambiguity).

Resource-based approach to strategic management is the pedigree of the related streams of thought, such as knowledge-based or competency-based thinking, which have become influential in recent years.

4.2 Background

The name of the investigated *German firm* (henceforth "investigated firm") is kept anonymous because of the non-disclosure settlements agreed among the actors. The number of employees of the investigated firm has more than doubled in the past three years. At the end of 2010 the organisation saw about 210 members of staff (Source: annual report of the investigated firm). The descriptions presented are based upon data elicited and analysed during a contracted project, for which the author was responsible. It took the project team approximately *three months* to complete the project.

Business routines and processes of the investigated firm are *supported by information technologies*. The *central IT tasks* include the provision of necessary software and hardware infrastructure for office-based automation and workforces, for functional and management information system at different organisational hierarchies, for Electronic Data Interchange (EDI) with external business partners, for telecommunications purposes, for external and internal websites.

The project *objective* was to improve the organisational and technical infrastructure aimed at improving protection and resistance against electronic *malware*. Information security comprises far more areas, but malware is an important subject in the field. The data about and surrounding this subject may provide details of *strategic resources* related to information security inside a firm. Malware are malicious software elements programmed to disrupt systems, deny operations or search for and exploit information that may lead to the loss of business secrecy or personal privacy and to other unlawful und immoral patterns of behaviour. Typical forms of malware include viruses, worms, trojan horses, rootkits, spyware, backdoor, dialler, scareware. The *trigger* of the project was a malware intrusion into the IT systems in the past, which caused infectious workstations, notebooks and other network elements. Significant loss of data and costly actions of recovery were the consequences.

Notably, there is a large base of highly *sensitive data* objects in terms of privacy, secrecy and importance that the investigated firm receives from external business partners and internally processes. Data and information security is an operational imperative for the investigated firm.

4.3 Methodology

The investigated firm was determined to improve the information security by accessing external expertise. The author and his team analysed the needs of the firm, responded to the *invitation of tender* and eventually became commissioned to carry out the project in 2011.

Essential project members then met at the premises of the investigated firm in an introductory session, in order to

initiate the project activities. The author's project team decided to base the analysis procedure upon the standards and norms established by the German Federal Office for Information Security (*BSI*), especially upon the so-called *IT-Grundschutz Catalogues*. This standard delineates the potential threats in different areas of information security and recommends corresponding security safeguards. Typical business processes, applications, systems and networks in information technologies are tackled by the Catalogues. Special needs and data objects of extremely high sensitivity can be treated in a risk analysis supplementary to the Catalogues. Notably, malware treatment is reified in depth in one of the modules in the Layer One of the Catalogues: B 1.6 "Computer virus protection concept", based upon which a detailed *questionnaire* was designed by the project team. The questions focused upon organisational and technical leaks inside the investigated firm, which may act as sources of threats and weaknesses and would course detrimental effects on information security. The questionnaire also enlisted support of knowledge stemming from another module in the Layer One of the Catalogues: B1.1.3 "Security awareness and training".

The *exploratory nature* of the intended study is obvious. The project team was keen to find out facts and practices taking place in the investigated firm, in order to identify the potential sources of failure. *Semi-structured interviews* can be highly effective for such studies. Designed questions had been treated in a number of *main vis-à-vis and complementary telephone interview sessions*. Each semi-structured face-to-face interview took approximately a working day for team members to accomplish. *Eight employees* of the investigated firm attended the interviews. Two of them belonged to the IT Department. Three came from the Department for Office Communication. These two departments are the supporting units related to information technologies. Other three interviewees represented *two functional departments*.

A special aspect is that the investigated firm has outsourced some IT issues, such as data backup and administration to an *external IT service provider* (henceforth "external service provider"). The service provider offers IT solutions to a number of customers and hosts a computer centre, which belongs to the investigated firm. There exists however no Service Level Agreements (SLA) between the investigated firm and external service provider. Server systems forming the computer centre were made available since 2008. The IT solutions for different customers of the external service provider had jointly consumed the same hardware systems before 2008. *Three employees* of the external service provider were confronted with the designed questionnaire.

4.4 Data

The essential findings of the interviews are summarised in the following tables:

Table 1. Organisational issues related to malware

Domains of questionnaire	Brief description of findings
Security concept against malware	• There is no such conceptual guideline available in the investigated firm. • No written concepts are available either in the computer centre hosted by the external service provider. • Some measures concerning access control can be found in the employee instruction of the investigated firm. • A systematic set of organisational or technical measures against malware does not exist in the investigated firm. • Employees of the investigated firm know implicitly, whom they may call when irregularities on their computers take place. • Concrete measures are taken on an ad-hoc basis. • The documentations are administrated in SharePoint by the investigated firm. Security aspects are not considered in the involved technical components. The processes of documentation management are roughly described in lists, but have not been specified in detail. A Configuration Management Database (CMDB) does not exist. • The external service provider contends that the major ITIL (Information Technology Infrastructure Library) processes do exist, including Configuration Management. • A number of data objects in the investigated firm are of high importance and sensitivity. The data processing does not provide differentiated protection mechanisms based upon

	the degree of data sensitivity.
Timeliness of antivirus (anti-malware) software	• Antivirus software is made available on the servers in the computer centre. The external service provider is responsible for the update of virus definition list and engine. Change management practices (change of software versions) organised by the external service provider do exist at the server side. • Antivirus software also exists on the workstations and notebooks (clients) of individual employees of the investigated firm. The Department of Office Communication is responsible for installing the up-to-date software. There is no test procedure available prior to the installation on clients. Change management practices do not exist. • Antivirus software is updated on an hourly basis at the server side by the external service provider. However, such programmes are installed without tests. • The timeliness of the antivirus software (engine and virus definition list) is verified only on newly purchased desktop computers or notebooks in the investigated firm. Devices already in operation are not checked at all. No update management has been established. • Concerning the antivirus software, patch and change management are only practised by the external service provider at the serve side, but not by the investigated firm on clients (desktop computers and notebooks).
Deployment of antivirus software	• Servers of the investigated firm are scanned each day by the external service provider. • Scans on the clients are not controlled and no rules exist. Individual employees are themselves responsible for keeping their computer "clean" and updating the antivirus software. • Nor are there rules and mechanisms in the investigated firm, based upon which virus scans are forced during a data exchange or transmission.
Administrative change	• Changes made by system administrators are documented (e.g. documentation about system maintenance tasks carried out by the administrator) by the external service provider for servers. Non-administrators are not allowed to enforce any changes on system. • Administrative changes are not in a controlled state on clients and not documented in the investigated firm. • The investigated firm intends to install a Document Management System (DMS), which should capture administrative changes on clients in written form in the future. • Email and web systems are also used for private purposes by employees of the investigated firm, although it is desirable to separate business and private usage.
Registration of incidents related to malware	• Documented rules of registration process and responsible persons do not explicitly exist in the investigated firm. However, implicit patterns of behaviour do exist. Employees would contact the Department for Office Communication while encountering incidents. • The Department for Office Communication does not received automatically generated messages from antivirus programmes upon incidents. The reasons are the improper configuration settings in the antivirus software, lack of access right to obtain the information or incompatibility of interacting software systems. • The registered incidents of the investigated firm are not prioritised according to their frequency of occurrence and business impacts.
Behavioural rules upon incidents related to malware	• No rules ensure that all identification data and passwords used by the computers are changed immediately after the infection occurs.
Regular Data backup	• No backup concept exists for client computers in the investigated firm. Individual employees are themselves responsible for local data. • The external service provider does backup server data on a regular basis.

Table 2. Technical issues related to malware

Domains of questionnaire	Brief description of findings
Security concept against malware	• Antivirus software reacts on demand and on access at the client side. Clients are also protected by the firewalls physically installed in the investigated firm. • Deployment of antivirus software is more structured at the server side (external service provider). Servers are grouped in different types, such as terminal, mail and file servers. • Client systems are using CA eTrust as the antivirus tool. ClamAV is employed to treat mails. ArpGuard has been protecting the firm's internal networks. Checkpoint is deployed as the firewall, and Window Firewall has been deactivated. • Server systems are protected by Trendmicro as the antivirus tool.
Prevention against malware	• There is no mechanism in the investigated firm to monitor and control if the antivirus software is really installed and updated on individual clients. • The external service provider updates the virus definition list hourly. • Data and programmes are not deliberately scanned prior to usage on clients. Client users reply on the automatic mechanisms of the antivirus software. • Data and programmes are deliberately scanned prior to usage on servers administrated by the external service provider. Data exchange or data integration on servers must be authorised by the investigated firm. Without such authorisation, the data transfer is rejected. • In the investigated firm, no administrator right for operation system is available for client users. Nor is local administrator right available for client users. Administrator rights may be allocated to users at the application-level. Additional rights are defined in the Active Directory for specific purposes and users, such as network printing tasks. However, there is no formal Identify and Access Management (IAM) system installed technically and organisationally. • In the investigated firm, existing administrator accounts are only used when for example programmes are to be installed on clients. However, there is no control mechanism for functional separation between administrator and normal accounts. • Neither the investigated firm nor the external service provider carried out the evaluation of firewall log files. An Intrusion Detection System (IDS) is not deployed either.
Selection of a suitable antivirus software	• A criterion set does not exist, based upon which the investigated firm can select suitable antivirus software. • The external service provider does select the antivirus software, using a number of criteria. However, these criteria are rather vague and informal than precisely formulated. • It is wished by the investigated firm to administrate the antivirus software on clients from a central computer. • In the investigated firm, not all the IT systems are protected by the deployed antivirus software currently. Systems such as iMac, iPhone or other smartphones are most probably not covered by the protection mechanisms. • Servers at the premises of the external service provider are better protected through its antivirus software, covering all typical file systems, data formats, archive formats and transmission protocols. • Potential malware residing in active content, such as ActiveX, JavaScript or Flash, is not sufficiently treated by the currently employed antivirus software, neither on servers nor on clients. There exists no Browser-Policy. • There is no information about the "health" of the antivirus software itself.
Update of deployed antivirus software	• The engine of the antivirus software is updated on the server when the regular maintenance is carried out weekly. • The virus definition list is updated each hour on the server. • Updates on clients are not controlled and no systematic information about the versions and

	update frequency is available.
Deployment of antivirus software	• The central e-mail gateway of the investigated firm is protected by antivirus software. • For Internet services of the investigated firm, there are a number of mechanisms used, such as blacklists and firewall rules. • Encrypted files are not sufficiently protected on clients. Users are acting individually. It is for example not ensured that an encrypted filed is scanned after decryption. • CA eTrust can be deactivated by client users while the deactivation of Trendmicro is protected by a master password.
BIOS security	• BIOS settings can be changed on elder client computers purchased before 2010. BIOS on newly purchased computers are protected by a password. • Client computers are first but not only booted from hard disk. • It is not tested and checked on clients if the configurations set in BIOS have become effective. • Virus warning in BIOS is not activated on clients.
Behavioural rules upon incidents related to malware	• Systems that are or supposed to be infected are powered off immediately. • Not all infected systems will be completely setup and configured from scratch again. Systems will be further used if the antivirus software does not make any notifications anymore after the infection treatment. • The act of disinfection is not recorded in written form. • Knowledge generated from incidents is not summarised and updated constantly in the investigated firm, while the external service provider does organise internal reviews and audits for knowledge management and documentation.
Creation of a Recovery Boot Medium	• A recovery copy does exist in form of images, which are updated quarterly and under certain necessary circumstances. However, the content of recovery is not defined formally in written form and only contains what the investigated firm perceives necessary. • The investigated firm creates different images for different client users. • The external service provider creates full images and backups weekly. • The investigated firm and external service provider both contend that all necessary programmes, drivers and data are on the images. • The investigated firm does not scan the content of the image prior to its creation, while the external service provider does. Both do not scan the image itself after its creation. • Images are kept on external hard disks in the investigated firm and not connected with other devices. The access to recovery medium is controlled. The external service provider creates images and backups on tapes, which are kept and managed by its external business partner.
Regular data backup	• The external service provider has developed a concept for the backup of all operational data of the investigated firm that cannot be derived from other sources of information. The investigated firm lacks a backup concept. • There are not practised rules that consider the availability requirements of the informational assets inside the firm. The external service provider treats the availability by measures such as creating images, RAID1 mirroring and tapes mirroring in different fire sections. • There are no practised procedures, neither by the investigated firm nor by the external service provider, which ensure that the defined or envisioned backup processes are carried out smoothly and secured data can be restored safely.
Handling of mobile data medium	• Used mobile medium by the investigated firm includes DVD, CD, USB sticks, flash cards, external hard disks, mobile phones. • The USB interfaces on computers and notebooks are not restricted for usage. • Optical drivers exist normally on computers and notebooks. They are not restricted for usage. The system can also be booted from the optical driver. • Data exchange through mobile data medium is carried out by individual employees of the

	investigated firm on client computers. The process is not controlled at all. • Data exchange though mobile data medium is strictly controlled by the external service provider at the server premises.

Elicited interview results stemming from different employees of the investigated firm and the external service provider are compared, aggregated, documented and analysed in various workshops organised by the project team. The standardised modules in the BSI Catalogues mentioned before formed the base of formulating *recommendations for improvement*. Response to the invitation to tender, questionnaire, interview data, data analysis, safeguard recommendations and implementation suggestions formed the base of the *project results and documentation*.

4.5 Discussion

The case of the investigated firm implies at least two major factors that make information security indispensable in today's business environment. First, information encompasses all informational assets of a firm, in information technologies as well as in other functional and supporting divisions and departments (see project background and methodology). *Identifying, categorising and prioritising* informational assets may be the first step of information security management. Second, the security of the informational assets is of general interest for top management and determines the "safety" of business operation at all management level (see project objective and trigger). No doubt, resources, tangible and intangible, that build, develop and optimise information security, have increasingly gained importance in businesses and are of *high value* to the investigated firm. Even in a firm located in a developed economy such as Germany information security is a relatively new "discipline". In-depth expertise is rather *rare*. An external specialised expert was consulted in the case of the investigated firm. The outsourcing of server administration that implicitly includes the data safety is another proof of the rarity of competencies in this area.

Resources related to information security cannot be installed over night. Especially the relevant intangible assets, such as knowledge and capability of learning in this area, are *accumulated consciously and difficult to imitate and substitute*. Interview data shows that investigated firm is still in its infancy as far as information security is concerned (see interview findings in almost all domains of questionnaire, especially "Handling of mobile data medium"; "BIOS security" and the treatment of antivirus software in interview findings). The medium-sized company has just begun to *become conscious* about the art of protecting its informational assets. The case also indicates that although the external service provider, a specialised IT company, has integrated a number of security practices to treat information (see e.g. "Regular data backup" in interview findings), the grasp on the issue is still loose (see e.g. "Behavioural rules upon incidents related to malware"; "Selection of a suitable antivirus software" in interview findings). A combination of an unfortunate threat and a relevant vulnerability would be sufficient to possibly cause detrimental business impacts. The case further implies that some security measures may exist in firms, but they come from operational needs rather than from strategic planning. *Concepts, policies, monitoring and controlling mechanisms* and *system of evolutionary improvements* lack significantly (see e.g. "Security concept against malware"; "Registration of incidents related to malware"). It seems to be a general phenomenon in the business reality that information security is reflex rather than strategy. Realisation of information security is often supported by investments in *software and hardware*, which are subject to substitution (different vendors, different tools). However, *knowledge* that constantly to be updated and *organisational agility* to plan and implement the new insights coming from the changing knowledge are not only difficult to imitate, but also can be *hardly substituted*.

The case study demonstrates forcefully that resources related to information security are of strategic nature and business strategy can benefit from fostering such resources. Results found and analyses conducted in the context of a specific firm have provided valuable knowledge about the status and direction of development of the security-related resources inside firms.

5. Market-Based Implications: Case Study of a National Market

Ginter and Duncan (1990) argued that while conducting the strategic analysis, it is necessary to scan, monitor, forecast and assess the market environment, which consists of a set of operational characteristics that a particular national marketplace possesses. Business firms can extract these characteristics by evaluating the (s)ocio-demographic, (p)olitical, (e)conomic, (n)atural environmental and (t)echnological factors existing in the national market. SPENT is thus an abbreviated form of the forces at work in the broad market. This section delineates issues related to information security in a chosen national market, Germany. Based upon the analysis,

strategic implications are then derived in a following discussion.

5.1 Socio-Demographic Factors

The significant socio-demographic phenomenon related to information security in Germany has been the rapidly increasing *societal consciousness* towards the protection of individuals' information. Increasing number of German citizens as well as profit-oriented and non-profit corporations have developed a stronger instinct towards *privacy and anonymity* in recent years, which has induced a more intense willingness of individuals to remain unnoticed or unidentified during the contact with other members and social entities. This kind of observations can be made across a *wide demographic spectrum*, including different professional and ethnical groupings, men or women, younger or elder, east or west in Germany, and, more or less educated stratum.

The traditional system of value, attitude and belief accompanied by *unprecedented progress in technological development* certainly has been playing a vital role in determining the trend of security awareness. Arguably, *Digitalisation* of the personal information, increased number of *information-based crimes* and transfer of relevant information and knowledge through *mass media*, such as Internet and television, have also contributed to the desire for more anonymity and become the primary drivers of informational thriftiness.

Much more personal information than ever before is considered as private, special and sensitive. The telecommunications vendor Nokia Siemens Networks commissioned a study recently, which investigates the status of consumer sensitivity in relation to personal information (Nokia Siemens Networks, 2011). The study interviewed five thousand (5, 000) individuals in five European nations. The study found that personal information such as names, photos and professions are increasingly recognized as a very sensitive piece of information and therefore worthy protecting against abuse and misuse. Particularly, eighty percent (80%) of the German interviewees stated that data protection has become an issue of high importance in their life; sixty three percent (63%) of the respondents in Germany were concerned about privacy violations and seventy four percent (74%) of them stated their high wariness at disclosing their personal data; the most sensitive data in the society is the credit card number (94%), financial standing of the person (90%) and personal photos (88%). The study also compares the same results with the findings of the previous year. Sixty seven percent (67%) of the interviewees stated that the information about their profession is sensitive in 2010, compared to forty one percent (41%) in 2009. Information about marital status was perceived as sensitive by fifty seven percent (57%) of the respondents in 2010, compared to thirty percent (30%) in 2009. This trend is evident also in other countries.

5.2 Political-Legal Factors

The efforts against unsanctioned invasion of anonymity by the government, corporations or individualsare a significant part of many countries' laws related to privacy and information security. Germany is no exception. The pressure of compliance to *national, subnational and supranational lawful regulations* is probably the most salient political factor relevant to information security.

The German Federal Data Protection Law (*BDSG*: "Bundesdatenschutzgesetz") is the overarching law at the national (federal) level that stipulates how the individual information of natural persons must be treated and protected. BDSG has evolved since 1970. An essential axiom of the law is the so-called principle of prohibition, meaning that the collection, processing and use of personal data are principally prohibited, which is only allowed if either an explicit legal arrangement is given or if the natural person concerned has explicitly, usually in written form, given their consent to the collection, processing and use (BDSG, 2009: §13, par. 2). Strengthened protection is provided to the so-called specific types of personal data, namely the information about racial and ethnic origin, political convictions, religious or philosophical beliefs, trade union membership, health and sexual life (BDSG, 2009: §3, par. 9). Notably, BDSG is based upon the Data Protection Directive *95/46/EG* published by the European Union in 1995.

BDSG interacts with other *specific legal enactments*, such as Telecommunications Law (TKG), Telemedia Law (TMG), Criminal Law (StGB), Works Constitution Law (BetrVG), Social Law (SGB), General Equal Treatment Law (AGG), Commercial Law (HGB), Canon Law (KiG), Nursing Home Law (HeimG), Hospital Laws of federal states, Registration Laws of federal states, Foreigners Law (AuslG). These specialised laws "collaborate" with BDSG so that specific security compliance issues in specific social, political and commercial areas and industries can be treated properly.

BDSG is applicable in private sector and governmental administrative bodies at the national level. *Data protection laws at the level of individual federal states* are responsible for regional, local and municipal security of personal data.

While BDSG and its related regulations are primarily concerned with data protection for *natural persons*, the

scope of information security is wider, encompassing the provision of data protection and IT risk management also to firms and organisations as *juristic persons*. Two important regulations in Germany need to be considered in this context, namely the so-called Generally Accepted Standards for Accounting Systems based on Data Processing (*GoBS*) and Principles of Data Access and Verifiability of Digital Documents (*GDPdU*).

Further relevant laws are Generally Accepted Accounting Principles (GoB), Tax Regulation (AO), Income Tax Law (EStG), Regulation of Implementing Salary Tax (LStDV), Balance Modernisation Law (BilMoG), Law on Limited Liability Companies (GmbHG) and Law on Control and Transparency in Business (KonTraG). Furthermore, the American standard Sarbanes-Oxley-Act (*SOX*) also plays a vital role in the management of information security in German firms and organisations.

5.3 Economic-Governmental Factors

Germany is the largest economy in Europe and fourth-largest economy in the world in 2010. The nation is notoriously strong in innovative and export industries, such as machine construction, automobile and household electronics, conferring a competitive position on the balance of payments of the nation. However, Germany lacks natural raw material and is an importer in this sector. Fiscal and monetary policies implemented at the European and national level in the past has been shaping Germany in many characteristic aspects of its national economy. As an industrialised nation Germany's economic growth rate is relatively low to moderate. Levels of income are relatively high. Productivity, especially in high-tech industries, is relatively high. Levels of inflation are low. Levels of unemployment vary in different economic cycles and stabilised at a low level most recently. Since the formation of the European Monetary Union Germany's export-centric economy has benefitted vastly from the introduction of Euro as the formal legal tender.

Surrounded by the broader national economic conditions, the German *fiscal policy* ("Bundeshaushalt") has continuously assigned and raised attention and vigilance to information security in recent years. Within the structure of the Federal Ministry of the Interior four distinct organisational units are completely or partly dedicated to the security in the information age.

The Federal Office for Information Security (*BSI*) investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions (BSI, 2009). Since its inception at the beginning of 1990s, the number of BSI's employees has more than doubled (BSI, 2010).

The National Cyber Defence Centre (*NCAZ*) is a German governmental agency established to respond to attacks on government computers in Germany. At the core of the cyber-security is the protection of critical infrastructures. Governmental entities and firms from the private sector are co-operating closely in this national project (BSI, 2011). NCAZ was found at the beginning of 2011 and is administratively controlled by BSI.

The Federal Commissioner for Data Protection and Freedom of Information (*BfDI*) originated in 1978 and is an independent authority for overseeing data protection by federal governmental and public agencies and by firms providing telecommunications and postal services (BfDI, 2009). This institution received 12.5 new staff positions in the fiscal year 2010 and number of staff rose from 69 to 81 between 2008 and 2010 (BfDI, 2010).

The Federal Office for the Protection of the Constitution (*BfV*) and its offices at the level of federal states have been tasked with the collection and analysis of information, intelligence and other documents concerning efforts directed against the free democratic basic order, against the existence and the security of the Federation or one of its states, and against the peaceful coexistence of peoples. It is also tasked with counter-intelligence, protective security and counter-sabotage (BfV, 2009). This institution was established in 1950. BfV has revealed recently that Germany's open and pluralistic society makes it easier for intelligence agencies to gather information. Some intelligence services are showing growing interest in intelligence targets in Germany's industry, research and technology. For this reason, it is important to raise awareness among businesses and research institutions and provide information about the threat of industrial espionage (BMI, 2010).

5.4 Natural-Environmental Factors

Natural environment may exert immense influence upon markets, thereby shaping products and businesses significantly. One major question is which kind of natural power may occur in the relevant national markets. Natural phenomena include not only normal parameters such as *weather, temperature and humidity* but also unpleasant *catastrophes* such as floods, hurricane, freezes, earthquakes, avalanches, volcano eruption and droughts. The other major question about natural environment which the strategists must be aware of is the *unpredictability* of natural events. *Probability* of occurrence is something too vague to be calculated precisely.

The "Federal Office of Civil Protection and Disaster Assistance" (*BBK*) in Germany is a central governmental

organisation responsible for civil security since 2004 and lists the most substantial natural catastrophes in the last ten years as follows:

Table 3. Most significant natural disasters in the last 10 years in Germany

Year	Event	Duration	Casualties / total estimated economic damage
2008	Hurricane Emma	February 29-March 02	14 dead, including 6 in Germany / approximately 1 billion Euro
2007	Hurricane Kyrill	January 18, 19	47 dead, including 13 in Germany / approximately 10 billion US$
2006	Flood of river Elbe	March-April	n/a
2005	Flood of the Alps	End of August-Beginning of September	at least 30 dead (all outside Germany) / approximately 4 billion Euro
2003	Heat wave	June, July, August, predominantly in the first half of August	23,000 cases resulting in death, including 3,500 in Germany / approximately 13 billion US$
2002	Flood of river Elbe	Mid-August	Approximately 18 billion Euro, including 13 billion Euro in Germany alone
2002	Hurricane Jeanett	October 27, 28	47 dead Europe-wide / approximately 1.7 billion Euro, including 660 million Euro in Germany alone
1999	Hurricane Lothar	December 26	110 dead, including 13 in Germany / insurance loss: more than 6 billion US$

Source: Adapted from BBK (2009).

The knowledge about the type of catastrophes, the probability of occurrence and the *resultant damage or loss* of information is of essential meaning for business strategy.

5.5 Technological Factors

Technological development in the last two to three decades, especially the development in information and communication technology (*ICT*), has revolutionised the way how businesses are conducted in an unprecedented way. Firm activities have generally become better co-ordinated, research and development is speeded up and many businesses have become much more flexible. In a developed market such as Germany, ICT has evolved to an indispensable base technology, based upon which products and processes in a wide range of other industries are designed and implemented.

As information processing is becoming increasingly electronic everywhere in the world, new kinds of ICT emerge quickly. Some state-of-the-art technologies that require careful security considerations are listed as follows:

- *Internet-based technologies* such as Networks, Clients, Emails, HTTP, VOIP, e-commerce, m-commerce are base technologies used in most organisations. These technologies are subject to significant security threats. The Open Web Application Security Project (*OWASP*) publishes the so-called top ten list periodically, revealing the most important web application weaknesses and recommending techniques for minimising operational risks;
- Most advanced Internet-based technologies such as *Cloud Computing and Web Services* as the business-enabler are among the most discussed topics in information technology. Putting sensitive information in clouds may necessitate significant knowledge in security controls and monitoring of access;
- Attacks in the *cyberspace* are threats to the data security of citizens, businesses and the government;
- *Digital ID* card (or *ePassport*) is introduced in a number of national markets, also in Germany. Unlike the current identity card, it is only the size of a credit or debit card and has a contactless chip. Securing the data on the card against malicious access and modification is a challenging tasks for both technicians and security managers;

- *E-government* activities are promoting the consistent use of modern ICT, integrating citizens and the economy in the governmental administration on the one hand, and organising the administrative processes more efficiently on the other. Authentication, certification, Public Key Infrastructure (PKI) and database safety are only a few significant security issues that may arise in such systems.

5.6 Discussion

While societies have been experiencing astounding speed of technological development in *digitalisation* and information processing, the *awareness* of information security and data protection has gradually become pervasive in firms and for individuals, especially in more developed markets. More mature the economy is, more tightly regulated is the information and data. Products and services must integrate *compliance requirements* according to national and supranational laws and regulations. Economic conditions in different markets shape the supply and demand differently, causing different design and implementation of products. Germany's increased *governmental investment* in public institutions related to information security indicates that at lease in developed economies public authorities and institutions have become more specialised in information security, providing information, knowledge and legal frameworks for technological innovations in public sector, private industries and consumer markets. Businesses that intend to avoid the loss or damage of information must evaluate the *natural environment and possible business impacts in the relevant markets* carefully. If threats and weaknesses are identified, firms must respond strategically, for example, in form of a *business continuity or contingency planning*. Furthermore, in a wide range of industries today, products and services themselves or the underlying processes enabling the products and services are technological innovations in *ICT*. Safeguard of information is a permanent unit of analysis in such a context.

The SPENT analysis shows that information security is exerting influences on all relevant forces in the market environment. Some of them are more general influences and some of them are more *market-specific*. Strategists should be aware of important security-related issues in different markets, while scanning the operational environment.

6. Industry-Based Implications: A General Analysis

Industry-based analysis encompasses actors and events which a business firm interact with directly. The firm both receives from and exerts on the industry influences. The most obvious actors here are suppliers, customers and competitors. Porter (1980) advanced an analytic model and argued that there are five significant forces that jointly determine the attractiveness of the industry to be investigated and firms should position themselves profitably. The *five forces framework* contains the power of suppliers, the power of buyers, the threat of new entrants to the industry, the threat of substitutes, and the rivalry among competitors in the industry. This section shall delineate each of the forces in turn. The following analysis does not concentrate on one certain industry, but on more general industrial issues from the perspective of information security.

6.1 The Bargaining Power of Suppliers

Information security may have neutral effects on the bargaining power of suppliers at first glance. The fact that a firm or an organisation emphasises security issues does not make a resource delivered by a supplier more or less scarce. Similarly, other key factors that determine the power of suppliers, such as the switching cost and substitutability of a resource, the variety of the industries served by a resource, the size of the resource supplier and the size of the resource purchaser, seem to remain unchanged, whether or not a firm is practising security policies.

Nonetheless, the electronic business-to-business and business-to-administration platforms deployed between suppliers and purchasers have gained importance in the daily business over the past decade. *E-business* is the conduct of transactions by means of electronic communications networks and applications. Firms are linking their internal and external processes more flexibly and operate more closely with each other to meet each other's needs and expectations. Customer Relationship Management (*CRM*) systems and Enterprise Resource Planning systems (*ERP*) for example integrate and automate the order, procurement and transport processes and add significant value for both suppliers and purchasers.

Electronic transactions with suppliers can help firms identify more upstream players across different industries and geographical locations on the one hand, and enhance the efficacy of the external procurement processes in resource markets and streamline internal value chain activities on the other.

One major hindrance of e-businesses has been the insufficiency of trust in technologies shared by the supplying and purchasing firms (Papazoglou & Ribbers, 2006). Firms strengthening the protection of informational assets can obtain considerable *confidence and trust* perceived by their upstream suppliers, which polishes the firm

reputation and makes the firm more attractive for its suppliers or potential suppliers.

6.2 The Bargaining Power of Buyers

Traditional factors affecting the bargaining power of buyers are not influenced by information security directly. The number of customers (buyers) and the quantity of purchase for example would not depend upon the existence of a firm's security policies. Neither would the industry concentration and size of the competitors nor the switching costs and availability of substitutes be immediately changed through considerations of information security. However, similar to the bargaining power of suppliers, firms are increasingly using e-business platforms to expand the geographical and industrial search of appropriate buyers in the electronic networks. The e-market would be perceived as being more attractive for buyers or potential buyers, if for example personal data, such as credit card number and delivery address, are kept and perceived as secure in transactions.

6.3 The Threat of New Entrants

On the one hand, the phenomenon of e-business has simplified the way how businesses are conducted, which has led to the fall of the entry threat in a variety of industries, particular in the more trade-oriented downstream businesses of the industrial supply chain.

One the other hand, introduction of the philosophy and practice related to the information security *raises the capital costs*. Forming a management system of information security internally and undergoing a certification process alone may incur intensive costs, without mentioning the investment costs in hardware, software and staff training. Firms that have built and implemented a security structure obviously are raising the cost of entry and may deter potential entrants more effectively in markets where information security in products and processes is crucial. Furthermore, as argued above information security may contribute positively to achieving distinctive reputation for existing players, thereby raising the height of the entry barrier additionally.

Special laws and compulsory compliance in particular industries also represent a significant barrier to entry. In Germany for example, telecommunications operators and vendors must abide by the rules related to information security in Telecommunications Law (TKG).

6.4 The Threat of Substitute Products

Information security may not be able to reduce the threat of potential substitute with lower price and improved performance, but can generate *customer (buyer) loyalty* through perceived security by the customers and through realised security by the seller, and thereby reducing the threat of substitution. Mobile phone conversations for example are protected against eavesdropping. Products with similar functionalities and lower prices can hardly become substitutes without similar security features and the same level of security perception by consumers. Many other industries impose similar user-driven requirements on products that prevent personal or transactional data from leaking. Furthermore, the efficiency gain achieved by engaging in secure e-businesses can also improve the *cost structure* of the firm on the long-term run, which makes the risk of a potential substitution even lower.

6.5 The Rivalry among Competitors

This force is, to some extent, related to the combination and interaction of the other four forces. High entry barriers and industry concentration for example may intensify the rivalry markedly. Strong buyers and existence of close substitutes may make the competitive pressure greater. Low switching cost and customer loyalty may induce high hostility among the industrial rivals. While formulating strategic issues, firms can enlist the support of information security to leverage mentioned competitive forces.

Notably, in today's Internetworking and information age, strategy aimed at protecting informational assets can deter *national or international rival espionage* in the industry more effectively and reinforce *patent &knowledge and quality& price advantages*.

6.6 Discussion

Firms organising around *e-business* can gain speed and time advantages in the *e-market*, which contributes to the reduction of the power of suppliers and buyers. Integration of security aspects in e-business improves the *confidence and trust* of a firm's suppliers and buyers. Thus, achieved higher volume of transactions in turn tends to reduce the power of suppliers and buyers. Firms qualified for *lawful compliance* and for *certified management systems* in information security can contend *higher reputation* perceived and raise the entry barriers, causing its competitors or potential entrants without such qualification operating at a disadvantage. Considering information security in business strategy can also potentially generate *buyers' loyalty*, reduce the risk of substitution and protect a firm's *intellectual property* more effectively.

7. Conceptual Synthesis

Recapitalising the essence of the preceding analysis the following figure proposes a conceptual framework to integrate information security in business strategy.

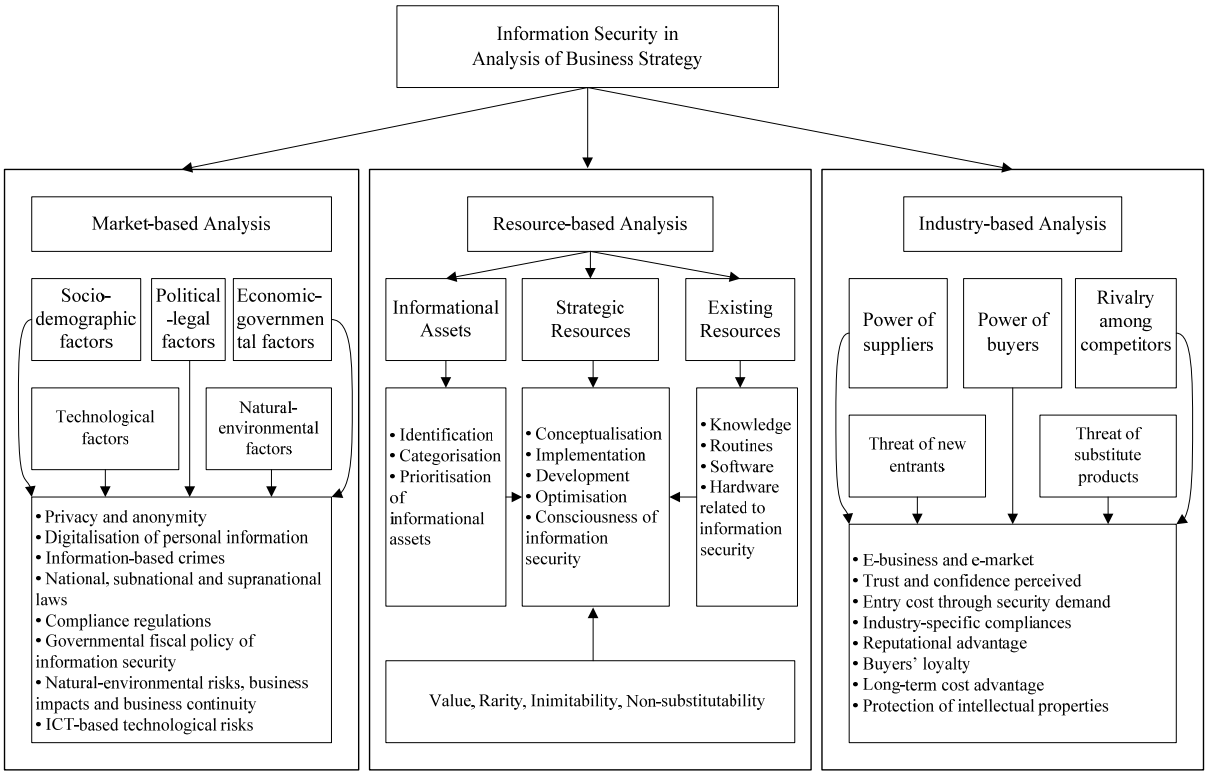

Figure 1. Incorporating information security in business strategy: a conceptual framework

Based upon this conceptual framework, the task of strategists is to collect and elicit information, in order to evaluate the external and internal issues related to information security. Strategic business units (SBUs) may benefit extensively from such strategic analysis, if key issues are identified appropriately. Solutions tackling these issues in form of *security strategies* (functional strategies of information security) are typically implemented within the *PDCA* cycle (Plan-Do-Check-Act). First, identified strategic issues and relevant risks are assessed and classified, treatment and methods of safeguards are planned carefully. The second stage includes the realisation, training and sensitisation of security concepts and measures. Third, incidents are detected and the effectiveness of the realised security measures is monitored and reported. The security system is then improved and made less vulnerable to technical and organisational errors. The PDCA cycle is a closed and recurring system with stages reinforcing each other.

Sources of knowledge for security strategies can be explored and exploited for example from a number of certification programmes, such as Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC) of Information Systems Audit and Control Association (ISACA); Certified Information Systems Security Professional (CISSP) of International Information Systems Security Certification Consortium (ISC2) as well as ISO 27001 Auditor. Software tools supporting the administration of security strategies and concepts are available in the market. The GSTOOL released by Bundesamt für Sicherheit in der Informationssicherheit (BSI) in Germany is one of such tools.

8. Conclusive Remarks and Further Studies

This paper is an attempt to incorporate information security in the analysis of business strategy. Especially the ubiquitous deployment of IT has made the security of informational assets indispensable to businesses.

The market-based strategic analysis puts emphasis on the national market and industrial circumstances external to a firm, while the resource-based approach examines inwardly the resources of a firm and their strategic characteristics. The article integrates these two views and investigates strategic implications of information

security from the perspective of resource, market and industry. The overall investigation encompasses an interview-based empirical case study conducted at a German firm, a SPENT evaluation focused on the national market environment in Germany and a more general industry analysis.

The insight generated from the investigation speaks an unambiguous language. The quality of strategy analysis benefits enormously from paying attention to information security. A conceptual framework synthesised from the results of the investigation argues that the deliberate inclusion of information security during strategic analysis can derive vital issues, based upon which part of the business strategy is developed, functionalised and implemented. The model also suggests a set of possible resource, market and industry issues that may be salient for business strategists generally. By having a close look at these issues businesses are able to embark on new opportunities, reinforce strengths, identify threats and deter weaknesses.

The applied approach in this article however suggests limitations of the conducted investigation and the direction of further studies. The firm case study examines only the state of information security at one point of time. Longitudinal case studies over a longer period of time and in different firms may deliver more comprehensive insights. Case studies may be carried out in different categories of economies (e.g. developed or newly industrialised economies), or in different cultural domains, in order to enable more reliable generalisations. The investigation of the role of information security may also enlist the support of cross-sectional quantitative studies, which control, confirm or falsify contended hypothesises. Furthermore, information security is an interdisciplinary subject. The first step of discussing information security in business strategy is the deliberate integration of knowledge in business & management and informatics & engineering.

References

Acedo, F. J., Barroso, C., & Galan, J. L. (2006). The Resource-Based Theory: Dissemination and main trends. *Strategic Management Journal, 27*(7), 621-636. http://dx.doi.org/10.1002/smj.532

Bain, J. S. (1959). *Industrial Organization.* New York: John Wiley & Sons.

Barney, J. (1986). Strategic factor markets: Expectations, luck, and business strategy. *Management Science, 32*(10), 1231-1241. http://dx.doi.org/10.1287/mnsc.32.10.1231

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99-120. http://dx.doi.org/10.1177/014920639101700108

Barney, J. (2002). *Gaining and sustaining competitive advantage* (2nd ed.). Prentice Hall, New Jersey.

BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe). (2009). Retrieved September 20, 2011, from http://www.bevoelkerungsschutz-portal.de/SharedDocs/Standardartikel/BVS/DE/ohneMarginalspalte/Naturkatastrophen/wesentl_Naturkatastrophen.html?nn=405216

BDSG. (2009). Bundesdatenschutzgesetz (German Federal Data Protection Law), German Federal Minstry of Justice, Berlin.

Besanko, D., Dranove, D., & Shanley, M. (1999). *Economics of Strategy* (2nd ed.). New York: John Wiley & Sons.

BfDI. (2010). Tätigkeitsbericht zum Datenschutz Tätigkeitsbericht für die Jahre 2009 und 2010, Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI), Bonn.

BfDI (Bundesbeauftragter für den Datenschutz und die Informationssicherheit). (2009). Retrieved September 16, 2011, from http://www.bmi.bund.de/EN/Ministerium/Beauftragte/BeaufDatenschutzInffrei/beaufdatenschutzinffrei_node.html

BfV (Bundesamt für Verfassungsschutz). (2009). Retrieved September 19, 2011, from http://www.verfassungsschutz.de/en/en_about_bfv/tasks.html

BMI. (2010). Annual Report on the Protection of the Constitution, Bundesministerium des Innern (BMI), Berlin.

Brenner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H., & Schaaf, T. (2011). *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung.* Carl Hanser Verlag, Munich.

BSI. (2010). Annual Report 2010, BSI, Bonn.

BSI (Bundesamt für Sicherheit in der Informationssicherheit). (2009). Retrieved September 16, 2011, from https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html

BSI (Bundesamt für Sicherheit in der Informationssicherheit). (2011). Retrieved September 19, 2011, from https://www.bsi.bund.de/DE/Themen/Cybersicherheit/cybersicherheit_node.html

Conner, K. R. (1991). A Historical Comparison of Resource-Based Theory and Five Schools of Thought Within Industrial Organization Economics: Do We Have a New Theory of the Firm? *Journal of Management, 17*(1), 121-54. http://dx.doi.org/10.1177/014920639101700109

Dierickx, I., & Cool, K. (1989). Asset stock accumulation and sustainability of competitive advantage. *Management Science, 35*(12), 1504-1511. http://dx.doi.org/10.1287/mnsc.35.12.1504

Eckert, C. (2009). IT-Sicherheit: Konzepte - Verfahren – Protokolle 6thedn, Oldenbourg Wissenschaftsverlag, Munich.

Freiling, J. (2001). Resource-based view und ökonomische Theorie: Grundlagen und Positionierung des Ressourcenansatzes, Deutscher Universität-Verlag, Wiesbaden.

Ginter, P. M., & Duncan, W. J. (1990). Macroenvironmental analysis for strategic management. *Long Range Planning, 23*(6), 91-100. http://dx.doi.org/10.1016/0024-6301(90)90106-E

Hagström, P., & Chandler, A. D. (1998). *Perspectives on Firm Dynamics, in: Chandler A D, Hagström P and Sölvell Ö (eds) The Dynamic Firm* (pp. 1-12). Oxford and New York: Oxford University Press.

Makhija, M. (2003). Comparing the resource-based and market-based views of the firm: empirical evidence form Czech privatization. *Strategic Management Journal, 24*(5), 433-451. http://dx.doi.org/10.1002/smj.304

Mason, E. (1949). The current state of the monopoly problem in the U.S.. *Harvard Law Review, 62*(6), 1265-1285.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). *Strategy Safari: A Guided Tour through the Wilds of Strategic Management.* New York: Free Press.

Nokia Siemens Networks. (2011). 'Europäische Vergleichsstudie zeigt: Deutsche sind weniger sicherheitssensitiv als ihre Nachbarn' Pressdd release presented at Mobile World Congress, Barcelona, Spain on Febuary 4, 2011.

Papazoglou, M. P., & Ribbers, P. M. A. (2006). *e-Business: Organizational and Technical Foundations.* Chichester: John Wiley & Sons.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: A resource-based view. *Strategic Management Journal, 14*(3), 179-191. http://dx.doi.org/10.1002/smj.4250140303

Peteraf, M. A., & Bergen, M. (2003). Scanning dynamic competitive landscapes: A market-based and resource-based framework. *Strategic Management Journal, 24*(10), 1027-1041. http://dx.doi.org/10.1002/smj.325

Porter, M. E. (1980). Competitive strategy: Techniques for analysing industries and competitors. New York: Free Press.

Porter, M. E. (1985). Competitive advantage: Creating and sustaining superior performance. New York and London: Free Press.

Prahalad, C. K., & Hamel, G. (1990). The core competencies of the corporation. *Harvard Business Review, 68*(3), 79-91.

Rumelt, R. P., Schendel, D. E., & Teece, D. J. (eds) (1994). *Fundamental issues in strategy: a research agenda.* Boston: Harvard Business School Press.

Sanchez, R., & Heene, A. (1997). *Competence-based Strategic Management: Concepts and Issues for Theory, Research, and Practice, in: Heene, A. and Sanchez, R. (eds) Competence-based Strategic Management* (pp. 3-42). Chichester: John Wiley & Sons.

Stalk, G., Evans, P., & Shulman, L. (1992). Competing on Capabilities. *Harvard Business Review, 70*(2), 57-69.