DOI: 10.17951/ijsr.2015.4.2.29

Finding the Right Balance Between Business and Information Security Priorities in Online Companies

Vasile Dorca
Technical University of Cluj-Napoca
vasile.dorca@ovi.com

Abstract
In order to keep up with the trend and satisfy the Internet users, it is crucial for the online businesses to adapt to new technologies and offer the right services (shop, bank online, etc.) to their customers.

To anticipate customer needs, the online businesses use customer behaviour analysis and process customer data. Even if companies handle customer information (e.g. PII is considered highly confidential and must be protected accordingly) to anticipate and meet customers' expectations, the management often struggles finding the right approach in making informed decisions when talking about information security of such data. This can threaten the sustainability of the business and put its customers at major risks (e.g. identity theft), risks that decision makers of companies do not see, or do not understand, the results being they do not invest properly to secure the data they handle.

This paper gives a parallel overview between:

a) the management priorities of an online business that handles customer data and
b) the implicit information technology and security threats that those priorities generate.

Once we have a view around point a) and point b), the paper will also show potential ways of finding a right balance between business needs, regulatory requirements and security of customer data so that the business can take risks to achieve their goals in an informed manner, using a customised risk assessment methodology, based on COBIT5 framework, industry leading standards and potential internal customised processes.

Keywords – customer data, information technology and security, sustainability, management.

1. Introduction

An online business (e-business) can be considered as any type of business activity that runs online, using the Internet.

With the advent of the Internet, online businesses started to develop and grow. People become busier and busier, so they try to be smart when spending their time. They use Internet to shop online, to bank online, to pay their debts, etc. In order to keep up with the trends, many „traditional" companies have adapted their business and developed new technologies, so they can offer their services online and make sure they develop and grow their companies (e.g. banking, offline selling shops, etc.). In the same time, other new companies have seen the huge opportunities that the Internet offers and they started exclusively online businesses to satisfy the Internet users/consumers (e.g. social media, blogs, online shopping, etc.).

As of 2014, the number of Internet users got to almost 3 billion, a wide variety of companies have decided that they must have an online presence in order to succeed.

Scope:

The scope of this article is to contribute to the actual knowledge in the risk management field by identifying the actual issues that companies have and define a useful framework for the Management and Information Security to rank their priorities according to the general and specific threats of the goals defined by the business (Kendler, 2013), (Maughan, 2014), (Kouns and Minoli, 2010), (ENISA, February 2007), (PWC, September 2013).

Objectives:

1. Identify the latest top priorities of an online business and the associated information security threats and risks.
2. Map the priorities and threats identified using different methodologies in order to be able to prioritise the business goals from an information security point of view.

Methodology:

1. Identify the latest top priorities of an online business and the associated information security threats and risks.

The online companies can have multiple business fronts that can be characterized by different types of categories. The most common business categories can be split into: Business Services, E-Commerce, Financial Services, Industry and Manufacturing, Internet and Computing, Retail and Shopping, Property and Accommodation, Travel and Transport, News and Media, Tourism and Vacations, Skills and Learning, Sports and Recreation, Free Business Listing (The Business Index, 2014).

According to a global survey conducted by *McKinsey & Company* in June 2014, it is getting clear that CEOs are getting more involved and playing an important role in the business digital initiatives. They realized that in order to grow the company they have to go digital. The investment and organizational structure has to support and facilitate the online growth. The top priorities of the executives in relation with the digital trends, showed in the survey are: **digital engagement of customers, digital Innovation of products, digital engagement of employees, big data and advanced analytics, digital customer-life-cycle management, automation**. To make sure all services of those priorities function 24/7 without interruptions, this goals determine a "must have" priority which is **availability** of all digital services and data (Gottlieb and Willmott, 2014).

Definitions:

Big data and advanced analytics – Big data and advanced analytics technologies support the business to manage large amounts of data they store, make a complex analysis and get real time integration and response from data in different systems/sources.

Digital Engagement of customers – "Managing digital engagement is all about managing the participatory power of millions of Internet users to profit your business" (Harden and Heyman 2009).
Automation – automation of manual tasks significantly helps companies to increase their efficiency by enabling faster delivery and reducing the risk of human error.
Availability – A literature review of ISACA, "Creating a Culture of Security", points out that the enterprises are highly dependent on information in function, and focus on uninterrupted on the availability of IT systems, ensure that data remains available within a reasonable period of time (ISACA, 2011).

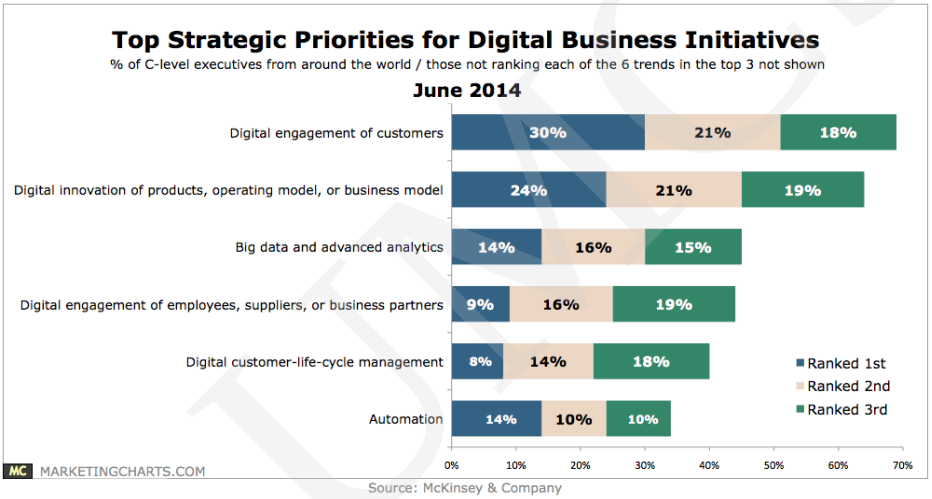

Figure 1.
Source: (Gottlieb and Willmott, 2014)

In order to achieve their goals through these priorities, companies often use **customer information,** such as Personally Identifiable Information (PII), or credit card information (PCI). This information is considered to be highly sensitive, as it can create damage to customers and implicitly to the company if it gets into the wrong hands, so the following topic that is going to be described and analysed in this paper is the **processing of sensitive information** that an e-business is using/owning.

A review of "Transforming Cybersecurity" book from ISACA, concludes that both sectors, business and private are becoming IT centric and majority of activities and transactions that used to be paperwork are now fully web-based. A few examples described include:

"**Banking and finance** — the proportion of electronic vs. traditional banking transactions is growing rapidly.

Shopping — web-based shopping is extended to new categories of high-value goods and services.

Travel and logistics — most booking, ticketing and reservation transactions are now done in an IT-centric mode.

Critical infrastructures — public services and corporate services deemed critical are pervasive and mostly IT-centric" (ISACA, 2013).

Conducting a focus group formed by experts in information security field and authors of this article, the above business categories have been structured based on the number of transactions they handle every day, the amount of sensitive data they handle and average number of customers. The data is shown in Table 1.

Business category	Criteria			Total
	Number of daily transactions	Amount of sensitive data handled	Number of customers	
Business Services	3	3	4	10
E-commerce	1	2	1	4
Financial Services	2	1	3	6
Industry and Manufacturing	10	11	10	31
Internet and Computing	6	4	6	16
Retail and Shopping	4	5	5	14
Property and Accommodation	13	10	13	36
Travel and Transport	7	7	7	21
News and Social Media	5	6	2	13
Tourism and Vacations	8	9	8	25
Skills and Learning	11	13	11	35
Sports and Recreation	9	8	9	26
Free Business Listing	12	12	12	36

Table 1.

Based on the above criteria, the business categories can be split as followed:

High	Medium	Low
E-commerce	Travel and Transport	Industry and Manufacturing
Financial Services	Tourism and Vacation	Skills and Learning
Business Services	Sports and Recreation	Free Business Listing
Retail and Shopping		Property and Accommodation
News and Social Media		
Internet and Computing		

1.1. The most common threats of an online business

Based on those four priorities that have been chosen to be analysed as being the top priorities for a digital business (big data and advanced analytics, digital engagement, automation and availability), the article is going to identify the most common threats that those priorities generate. The companies in scope for this analysis are only the companies that use customer data (PII + PCI), or any other sensitive data that can create a competitive advantage for each individual company (e.g. unlaunched products, in innovative products, secret recipes, etc.).

In this article are identified only the **Information security threats and risks** that can have an impact on:

- the confidentiality or integrity of information of value to the company; or
- the availability of such information due to a malicious threat.

All other risk types (e.g. Strategic, Financial, Commercial, Operational, People Risks) are outside of the scope of this article (Betfair LTD, 2014).

Generally, the information security controls should be driven by the threats identified according to the business profile and goals. Risks do not exist if threats do not exist and risks do not exists if vulnerabilities do not exist, so in order implement a risk-based approach in terms of information security, the threats should drive the information security priorities. In the next chapter, potential threats will be identified based on the top priorities of an online business, using different methodologies, so at the end businesses can take conscious and informed decisions about the risks they are facing and decisions they need to make about those priorities in order to achieve the business goals.

2. Map the priorities and threats identified using different methodologies in order to be able to prioritise the business goals from an information security point of view

2.1. Engagement questionaire mapping

Good practices in the industry encourage the Information Security team to get involved in all goals set by the company or any project from the inception phase. Companies' goals have different impact on security and a good starting point on defining the prioritisation of the goals is using an Engagement Methodology by answering different questions related to: data used, exposure and control of the data. The questionnaire is meant to do a first filtering of the priorities and identify the areas of potential security input needed. The engagement questionnaire has been built using the expertise of the authors in the IT security field. It is presented below in Table 2.

Engagement Questionnaire				Business Priority response			
Question	**High**	**Medium**	**Low**	**Digital Engagement**	**Big Data**	**Automa-tion**	**Availa-bility**
Does the priority introduce or change the handling of, or storage of, any sensitive information?	Changes sensitive data processing or storage, or gathers new sensitive information not already captured by the business.	Changes will be made to processing or storage of sensitive information as already exists, but no new sensitive information will be gathered.	No sensitive information is utilised or stored.	H	M	M	M
Will any data be stored or processed externally?	Yes, the priority involves the external storage or processing of sensitive information with a new provider.	Yes, the priority involves the storage or processing of non-sensitive or sensitive information with a known (approved/ tested) provider.	No, the priority does not involve the external storage or processing of any business data.	H	H	M	H
Could unavailability of information or systems related to this priority result in damage to the business?	Unavailability of information or systems could result in significant damage to the business (e.g. over £….k loss of revenue, significant reduction in share price, extensive negative international media coverage).	Unavailability of information or systems could result in moderate damage to the business if exploited (e.g. £…k-£…k loss of revenue, extended negative local media coverage).	Unavailability of information or systems could result in minor damage to the business if exploited (e.g. less than £…k loss of revenue, letters to local industry press).	H	H	H	H
Does the priority change or introduce customer-facing systems/services, or have potential impact to other business customer-facing services?	The priority will directly change or introduce new customer-facing systems/services and/or customer administration systems.	The priority does not directly change or introduce new customer-facing systems/services or customer administration, but other business customer-facing services could be affected.	No customer-facing systems or services could be affected.	H	M	M	L
Does this priority introduce a new critical system or modify interaction with any existing critical systems?	The priority will introduce a new critical system or significantly changes interaction with existing critical systems.	The solution will introduce minor changes to existing interaction with critical systems.	The solution does not introduce or modify interaction with critical systems.	H	H	H	H

Table 2.

Engagement Questionnaire				Business Priority response			
Question	High	Medium	Low	Digital Engagement	Big Data	Automa-tion	Availa-bility
Does the priority involve developing new components or introducing new technologies?	Little (or no) re-use of existing components / extensive development or introduction of new components and technologies.	Some re-use of existing components / moderate new functionality or technology.	Significant (or complete) re-use of existing components / minor new functionality; or no new components / technologies.	H	H	H	M
Are you using suppliers for development, data analysis, hosting or operations / support?	New suppliers will be used for development, data analysis, hosting or operations / support?	Existing suppliers will provide new services to the business.	Existing suppliers will provide services already being supplied to the business or no suppliers used.	H	H	H	H
Are there any other aspects of the priority that you think might have security implications (e.g. relating to potential loss of confidentiality or integrity of valuable information)?							
Top score priorities:				1	2	3	4

Table 2. Continuation

Source: (Betfair LTD, 2014)

Note: When completing the Engagement Questionnaire, "the worst case scenario" ratings have been considered.
Note: The total score has been rated based on the highest ratings received by the priorities in comparison.
Conclusion: based on the Engagement Questionnaire, the most relevant priorities from a security point of view, are classified as followed:
a) Digital Engagement, b) Big Data and Advanced Analytics, c) Automation, d) Availability

2.2. ISO 27005 Threats mapping

Once the first engagement has been done and there is a high level view of each goal, the next step would be to get a better understanding around the threats those goals can generate. Two standards have been used to map the threats with the goals defined: ISO27005 and ISO27001 as presented in Figure 2.

General threats: According to ISO27005, the threat model defined is structured as below:

Threats: physical damage (e.g. fire), natural events (e.g. weather), loss of essential services (e.g. loss of power supply), compromise of information (e.g. theft of media or documents), technical failures (e.g. equipment failure), unauthorised actions (e.g. unauthorised use of equipment), compromise of functions (e.g. abuse of rights, breach of personnel availability)

Origin of threat – threat actors (according to ISO27005): hacker, cracker, computer criminal, terrorist, industrial espionage (intelligence, companies, foreign governments, other government interests), Insiders (poorly trained, disgruntled, malicious, negligent, dishonest or terminated employees) (ISO27005).

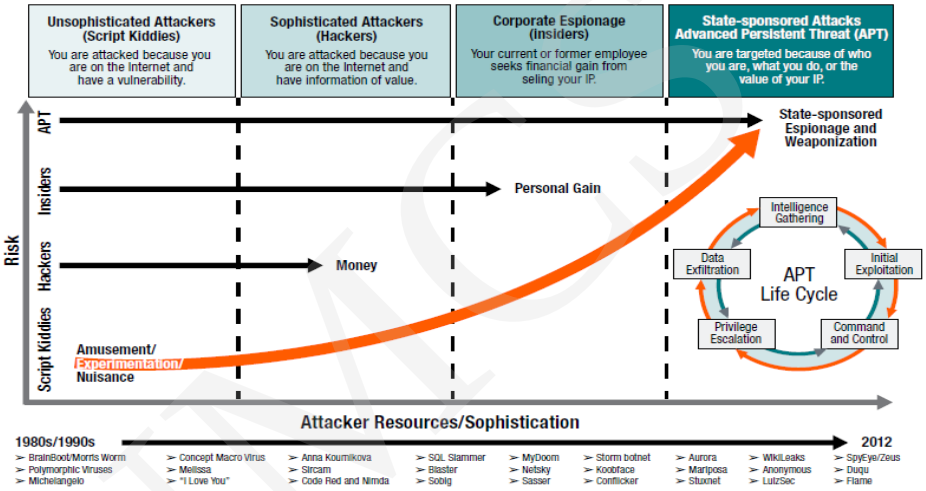

Figure 2.
(ISACA, 2013)

Source: ISACA, *Responding to Targeted Cyberattacks*, USA, 2013, figure 2

By mapping the ISO27005 threats with the business goals identified above, we can identify which are the most risky from an information security stand point.

2.2.1. Map the ISO 27005 General threats with the four business priorities:

Business Priorities	General Threats
Digital engagement of customers	• Unauthorised actions (e.g. unauthorised use of equipment) *Digital customers' engagement comes with storing and processing of PII (e.g. shopping offline vs. online store)*
Big data and advanced analytics	• Compromise of functions (e.g. abuse of rights, breach of personnel availability) • Compromise of information (e.g. theft of media or documents) *Big data and advanced analytics comes with increasing access to customer data to un-technical teams (e.g. marketing team)*
Automation	• No threats identified
Availability of services	• Technical failures (e.g. equipment failure) • Loss of essential services (e.g. loss of power supply) • Natural events (e.g. climatic) • Physical damage (e.g. fire)

Table 3.

By doing the threat mapping with the ISO standards, the conclusion highlights that the **Availability** generates the most threats, followed by **Big Data and Advanced Analytics**.

Digital Customers' Engagement comes as an inherent threat, due to the PII data handling, so based on the ISO27005 general threat model, the order of the four goals are:
a) Availability, b) Digital Engagement, c) Big Data and advanced analytics, d) Automation

2.2.2. Map the ISO 27005 Origin of threats with the four business priorities:

Business Priorities	Origin of Threats (threats actors)
Digital engagement of customers	Digital customers' engagement comes with storing and processing PII (e.g. shopping offline vs. online store), so this can be threaten by: • Hacker, cracker • Computer criminal • Industrial espionage (Intelligence, companies, foreign governments, other government interests) • Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)
Big data and advanced analytics	Big data and advanced analytics comes with increasing access to customer data to not technical teams: • Hacker, cracker • Computer criminal • Terrorist • Industrial espionage (Intelligence, companies, foreign governments, other government interests) • Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)
Automation	• Hacker, cracker, insiders
Availability of services	• Hacker, cracker • Computer criminal • Terrorist • Industrial espionage (Intelligence, companies, foreign governments, other government interests) • Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)

Table 4.

As we can see above, all threat actors can have a negative impact on all four priorities, meaning that all four priorities have the same importance for security.

A general conclusion after doing the mapping against ISO27005 threat model is that in order to make sure companies can achieve their goals through this priorities, the most „relevant" priorities from an information security point of view are **Availability** of services and **Big Data and Advanced Analysis**. **Digital Engagement** of customers comes with an inherent risk by "collecting" PII data when engaging customers online, therefore, the final proposed order based on the ISO27005 mapping is:
Availability, Big Data and Advanced Analytics, Digital Engagement and Automation

2.3. COBIT5 Mapping

"Information is a key resource for all enterprises. From the time information is created to the moment it is destroyed, technology plays a significant role in containing, distributing and analysing information. Technology is increasingly advanced and has become pervasive in enterprises and the social, public and business environments.

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information technology (IT). Simply stated, COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility and considering the IT-related interests of internal and external stakeholders" (COBIT Online, 2014).

"The main drivers for risk management in its different forms include the need to improve business outcomes, decision making and overall strategy by providing:

- Stakeholders with substantiated and consistent opinions on the current state of risk throughout the enterprise
- Guidance on how to manage the risk to levels within the risk appetite of the enterprise
- Guidance on how to set up the appropriate risk culture for the enterprise
- Wherever possible, quantitative risk assessments that enable stakeholders to consider the cost of mitigation and the required resources against the loss exposure" (COBIT Online, 2014).•

In the next chapter, the research will focus on the "quantitative risk assessments that enable stakeholders to consider the cost of mitigation and the required resources against the loss exposure" (ibid.).

From the COBIT5 framework we have chosen to do use 2 criterial selections to map with the four business goals:

– Vulnerability, Threat Risk and Impact
– Legal and Compliance

2.3.1. Map the COBIT5 Vulnerability, Threat, Risk and Impact with the four business priorities:

Using the same focus group, an analysis has been done to identify the Risk and Impact of the business goals, using the Threats and Vulnerabilities defined in COBIT 5 framework. The rating has been defined as High, Medium or Low, depending on the Impact and the probability that each risk can have.

The results show that according to the 10 vulnerability scenarios defined by COBIT 5 mapping and the threats, the **a) Big Data and Advanced Analysis** goal has the biggest Risk and Impact, followed consecutively by **b) Digital Engagement, c) Availability and d) Automation.**

Vulnerability	Threat	Risk And Impact	Digital Engagement	Big Data	Automa-tion	Availa-bility
Spear phishing	Attackers may gain access through phish payload or combined social-technical follow-up.	Initial data loss or leakage leading to secondary financial and operational impact	H	H	L	L
Water holing	Attackers may gain control of attractive websites and subsequent control of visitors.	Initial behavioral errors leading to secondary financial and operational impact.	H	H	L	L
Wireless/mobile APT	Attacks may compromise wireless channels and/or mobile devices to enable temporary or permanent control.	Partial or full control of one or more wireless installations and/or mobile devices; direct or indirect impact on all critical IT applications and services	M	M	M	M
Zero-day	Attacks use zero-day exploits to circumvent existing defenses.	Partial or full control of applications and underlying systems/ infrastructure leading to secondary operational impact.	M	H	L	H
Excessive privilege	Inside attacks may happen when inappropriate privileges and access rights are used.	Full and (technically) legitimate control outside the boundaries of organizational GRC, secondary financial, operational and reputational impacts.	H	H	H	L
Social engineering	Attackers exploit social vulnerabilities to gain access to information and/ or systems.	Partial or full control of human target(s), subsequent compromise of IT side, secondary impacts on personal/individual well-being.	H	M	M	L
Home user APT	Attacks use the fact that home environments may be less protected than organizational environments.	Partial or full control of applications, systems and home infrastructures, secondary financial, operational and reputational impacts, including impacts on personal/individual well-being.	H	H	M	M
Extended IT infrastructure APT	Attacks may target the IT infrastructure underlying critical organizational processes.	Full control of infrastructure, risk of extended control, including public infrastructures or business partners.	M	H	H	H
Non-IT technical infrastructure APT	Attacks may tunnel the barrier between IT and other critical infrastructures within the enterprise.	Partial or full control of nonstandard IT and technical infrastructure, e.g., supervisory control and data acquisition (SCADA), secondary operational impact.	M	H	H	H
Vendor/business partner exploit	Attacks on trusted business partners or vendors, compromising key software or deliverables.	Initial attack through organizational IT directed at third parties, with financial, operational and reputational impact.	H	H	M	H

Table 5.

2.3.2. Map the Legal and Compliance requirements with the four business priorities:

While doing a research around the legal and regulatory compliance in the information security field, it has been found that there are a couple of relevant certifications for digital businesses. The most important one for the financial services and businesses that handle cardholder data is PCI-DSS. Others to be mentioned and to consider when defining the business goals are: Sarbanes-Oxley (SOX), ISAE 3402, or National Security Strategies. Until now, there have been efforts in this field and a few examples to be mentioned are cyber laws and behaviour in cyber space, creating strategies to secure critical national infrastructure, or public and private sectors agreeing on legal and regulatory requirements. Even though those efforts bring value in the cyber space, there is a continuous improvement trend due to the more complex and advanced threats in this field, therefore, a few initiatives can be considered necessary to keep track with the threats: global interdiction of cybercriminal "safe havens" – combat Fraudonomics (FaaS), establish a supranational legal structure to enforce cyber security laws and a cyber-tribunal, or implementation of the national security strategies (e.g. US since 2003, Council of Europe Convention on Cybercrime 2004). In regards to the business priorities that are analysed in this paper, **Digital Engagement** and **Big Data & Advanced Analysis** are considered subject for more detailed analysis, as digital engagements may involve different countries or jurisdictions and Big Data involves storage of/access to sensitive information in different locations with different legislations (COBIT).

3. Conclusions

The research analyses the top strategic priorities of a digital business by using a focus group formed by experts in Information Security and the authors of this paper. The proposed framework has been built based on the experience accumulated by the authors during the years of experience and information security standards (ISO27005), best practices (COBIT 5) and legal and compliance requirements.

The research gives a parallel overview around the management priorities of businesses and the implicit information security threats that those priorities generate. Each business priority can be analysed from an information security perspective using the proposed methodology: getting a better understanding around the goal, mapping it using the usual methods of the Information Security Management System and identifying the most relevant threats to the specific goal.

The research highlights the importance of having a framework containing internal customised processes, industry leading methodologies, certifications and regulatory and compliance requirements. Each of the sources bring different aspects that need to be considered when defining the business goals. The advantage of the presented approach and framework is also confirmed in the results of the analysis that showed that when mapping the threats with the goals (ISO27005), availability of the services is the most impacted, while mapping them using an industry best practice, the results are different, as Big Data and Advanced Analysis takes priority.

By using the proposed framework when defining goals and priorities, the companies can take informed decisions about the risks they face in relation with the goals defined and the Information Security strategy can be built based on the results that the framework generates.

The research can be applied in practice for any priorities that the business can set and can give good indicators around the risks the company might face with their strategy. It is crucial for the success of the businesses goals to use methodologies that supports the decision making, so this research can provide a good linkage/bridge between the business management and information security.

The paper can be further explored and researched by finding methodologies of defining an Information Security Strategy using the presented approach. The research can also be a starting point in creating an automatic framework that can be used by the management of a business and by the information security professionals.

References

Betfair LTD (2014). Risk Taxonomy. London, UK.

Betfair LTD (2014). Security Engagement Form. London, UK.

COBIT (n.d.). COBIT Framework Usage. In COBIT.

COBIT Online (2014). *COBITONLINE*. Retrieved from https://cobitonline.isaca.org/l3-main?book=risk#risk-preface01-section03

ENISA (February 2007). *Information Package for SMEs, with examples of Risk Assessment/Risk Management for two SMEs.* Technical Department of ENISA.

ISACA (2011). *Creating a Culture of Security.* ISACA.ORG.

ISACA (2013). *Responding to Targeted Cyberattacks.* USA: ISACA.

ISACA (2013). *Transforming Cyber Security.* ISACA.ORG.

ISO27005 (n.d.). Information Security Risk Management.

Kouns, J. and Minoli, D. (2010). *Information Technology Risk Management in Enterprise Environments.* New Jersey.

Gottlieb J., Willmott, P. (2014, June). *McKinsey's*. Retrieved from http://www.mckinsey.com/insights/business_technology/The_digital_tipping_point_McKinsey_Global_Survey_results?cid=other-eml-nsl-mip-mck-oth-1407

Kendler, P. B. (2013). Retail IT Security Challenges.

Harden, L. and Heyman, B. (2009). *Digital Engagement – Internet Marketing That Captures Customers and Builds Intense Brand Loyalty.* American Management Association.

Maughan, D. (2014). DHS S&T Cyber Security R&D Programs.

PWC (September 2013). Key findings from The Global State of Information Security Survey 2014.

The Business Index (2014). *www.thebusinessindex.com*. Retrieved from http://www.thebusinessindex.com/categories/business-directory.aspx