MYKOLAS ROMERIS UNIVERSITY

BUSINESS AND MEDIA SCHOOL (BMS)

TOMAS MOGODIA

E-BUSINESS MANAGEMENT

INFORMATION SECURITY MANAGEMENT IN E-BUSINESS

Master Thesis

Supervisor

prof. dr. Darius ŠTITILIS

Vilnius
2016

TABLE OF CONTENTS

LIST OF FIGURES 3
LIST OF TABLES 4
INTRODUCTION 5
1. DEFINITIONS OF INFORMATION SECURITY AND E-BUSINESS 9
1.1 Information security management 9
1.2 Information security risk management 10
1.3 Information security incident management 12
1.4 E-business 14
2. INFORMATION SECURITY MANAGEMENT 17
2.1 Information security management models for e-business 17
2.2 Information security strategy for e-business 21
2.3 Information security architecture for e-business 24
2.4 Information security processes for e-business 30
3. RESEARCH METHODOLOGY FOR THE RESEARCH 35
3.1 Model for scientific empirical research methodology 35
3.1.1 Stage 1: Clarifying the Research Question 36
3.1.2 Stage 2: Proposing Research 38
3.1.3 Stage 3: Designing the Research Project 39
3.1.4 Stage 4: Data Collection and Preparation 40
3.1.5 Stage 5: Data Analysis and Interpretation 42
3.1.6 Stage 6: Reporting the Results 43
4. A CASE STUDY 43
4.1. Background for the case 43
4.2. Presentation of the case enterprise 44
4.3. Information security management 45
4.4. IT Security management 47
4.6. Information security procedures implemented in the organization 48
4.7. Information security breaches 50
5. INTERVIEW RESEARCH 51
5.1. Summary of results 58
CONCLUSIONS 59
REFERENCES 62
SUMMARY IN ENGLISH 66
SUMMARY IN LITHUANIAN 67
SUPPLEMENT 68
A. Interview questionnaire in English 68

LIST OF FIGURES

Figure 1 Number of Incidents and Number of Records 6
Figure 2 Scientific research outline 8
Figure 3 Relationship between information security and other security domains 10
Figure 4 Risk management 11
Figure 5 Incident management process flow 14
Figure 6 e-business application framework 16
Figure 7 Components of information security 18
Figure 8 The scope of strategy management 22
Figure 9 A Strategic Framework for Effective Information Security 24
Figure 10 Basic architecture of an information security management system 25
Figure 11 The SABSA® Matrix for security architecture 26
Figure 12 Leveraging COBIT to Implement Information Security 27
Figure 13 TISA: Layered trust information security architecture 30
Figure 14 Service design – the detailed picture 34
Figure 15 Formulating the research question 38
Figure 16 Data Preparation in the Research Process 42
Figure 17 Responders position in their organisations 52
Figure 18 Responder's organisations dependence to E-business 53
Figure 19 Responders possession of a degree in Information Systems or Telecommunications 53
Figure 20 Information leakages which occurred in the responders organisations 53
Figure 21 Usage of ITIL framework in responder's organisations 54
Figure 22 Frequency of risk assessment execution in a organisation 56
Figure 23 Incident management implementation in responder's organisations 56
Figure 24 Security incident management as a part of incident management in responder's 57
Figure 25 Organisations which have implemented security standards ISO 27000 and 27001 58

LIST OF TABLES

Table 1 Amount of employees in the responder's organisation 52
Table 2 Responders noted information security breach reasons 54
Table 3 Evaluation of technical knowledge needed to execute special functions 55
Table 4 Evaluation of importance of difference aspects while creating an information security strategy 57

INTRODUCTION

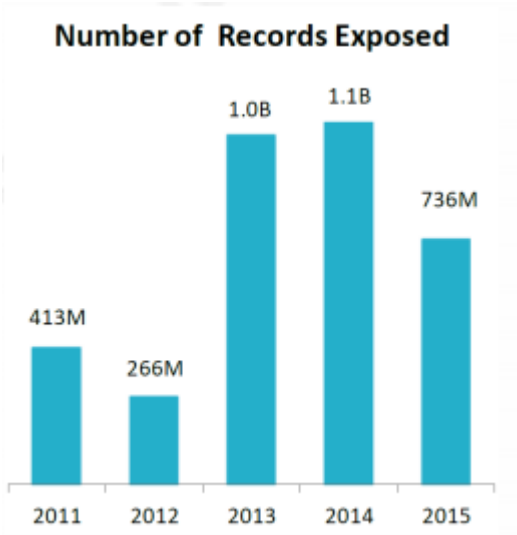
Relevance of the research. The topic of this master thesis will be of both theoretical and practical importance. Due to the examination of both theoretical and practical points of view on information security, the author will generate new ground and knowledge which may be used by future researchers for further investigation of the subject matter. Author would like to note that major impact in information security research was done by known researchers and organizations like Dan Geer (two of his most significant works are "Economics & Strategies of Data Security" and "System Security: A Management Perspective"), Gideon I. Gartner (founder of Gartner group) and NATO cooperative cyber defence centre of excellence in Tallinn, Estonia. Known researchers have investigated information security from the technician's point of view (cybersecurity implementation) and only partly investigated the management processes of information security management and never oriented in e-business type of organizations, while the world renowned Centre of cyber defence in Estonia is stressing the legal aspects of cybersecurity. Author will research the processes on the management level which have to be implemented to achieve a secure e-business (where cybersecurity from the technical point of view is one of the sub processes of information security management).

In the last decade information security management has become a more important issue for most large companies around the world. International businesses have also understood that better security cannot be achieved by just installing another security hardware device like a firewall or an intrusion protection system. Even the most secure system would not provide any security if the personnel operating sensitive information in the company is ready to reveal or steal it for personal reasons. It is a common understanding that information security heavily depends on the behaviour of the employees. Relevance of this scientific research is very important while considering the background in which E-business is operating in the XXI century and the risks that information leakages bring to business reliability and reputation. Looking forward to the most notable information thefts in last decade we can see that the biggest damage in public sector was done by authorised personnel stealing classified information from the employer – Edward Snowden case when 29-year-old Edward Snowden stole from the National Security Agency (NSA) 1.5 million of documents *[29, p. 1]* and more noticeable information thefts – the WikiLeaks, an enormous leakage of classified information which happened starting from 2007 and lasts until today publishing new confidential information to the public *[64]*. WikiLeaks will be the single case study from point view of United States of America National security agency's (NSA) information security management perspective, while NSA budget is approximately 10 billion dollars per year *[56]* – a single person could steal approximately 750 000 sheets of classified documents *[41]*. The case study will give a more in depth analysis of poor information security management even at organizations with enormous budgets as NSA. To supplement the research conducted in the case study there will be an interview of

information security professionals who lead information security segment in large international companies based in Lithuania a European Union.

In the XXI century, new technologies and telecommunication networks are continually emerging and leading to new methods of executing businesses worldwide. Mostly, this processes oblige any type of businesses to renew themselves by using new technologies to be prepared for new markets and business trends. As businesses increasingly depend on electronic data and computer networks to conduct their daily operations, growing pools of personal and financial information are being transferred and stored online. This can leave individuals exposed to privacy violations and financial institutions and other businesses exposed to potentially enormous liability, if and when a breach in data security occurs. Based on Insurance information institute in the USA number of data breaches and records exposed in 2015 in USA was an astonishing 781 million breaches with 169 million records exposed *[9]*. Following SANS institute bulletins of exposed information during the period from January 2011 to December 2015, the number of exposed records jumped from 413 million to 736 million per year, with 2013 and 2014 having over 2 billion records exposed *[7]*.

Figure 1 Number of Incidents and Number of Records



Source: Sans org. title: Building a Forensically Capable Network Infrastructure [7, p. 2]

Gartner predicts that "by 2018, the need to prevent data breaches from public clouds will drive 20% of organizations to develop data security governance programs" *[55]*. Author will concentrate on E-business information security management with concentration on information security models which have to be imbedded in the e-business architecture.

Author will investigate the root causes that have influenced the data integrity breaches and organizational processes which occurred (by conducting a single case study) and how did they impact the information security management process. As cyber security is integral with information security – author will not concentrate on cyber security (which are mainly practical technical processes) but will investigate information security in general (procedures, processes, physical security) with

adapting the processes to an e-business environment. Author will conduct an interview of leading Lithuanian and international information security experts and present an information security assurance model which is based on best practices (from a theoretical point of view) and from practical based on the conducted interview.

Research object. Information security management assurance in E-business.

Research problem. Researching the field of information security author investigated many guidelines and frameworks, but they were either very specific to technical implementation, either not adjusted to e-business. Scientific literature has huge amount of information about information security management practices (in general) but this knowledge is often purely theoretical or not adjusted e-business needs. This may lead that E-business will not understand the processes they have to implement and in fact this leads that proper processes in companies/organisations management may be absent.

Scientific research purpose. Analyse current information security management best practises used by businesses (which are indicated as industry standards) and based on information security experts interview and a single case study distinguish a principals for E-business companies to improve information security.

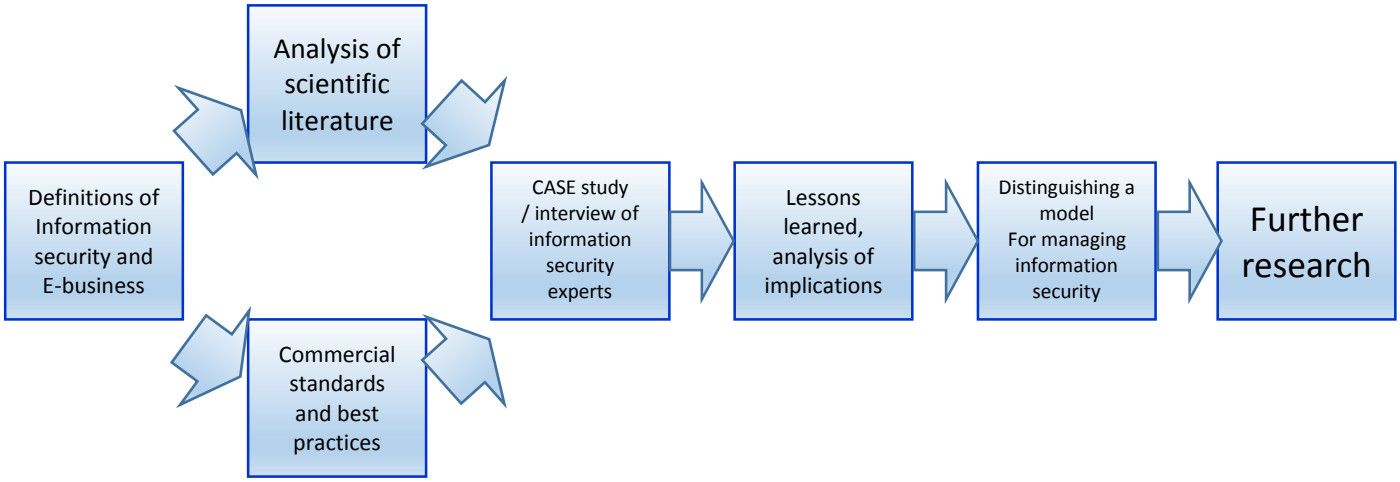
Hypothesis.

1. Information security management deficiency in E-business leads to loss of sensitive information.
2. Lack of information security management techniques leads to a lack of effective incident management.

The main objectives:

1. Analyse definitions of information security and E-business;
2. Analyse theoretical aspects of information security management in e-business;
3. Examine international standards and best practices on information security management;
4. Conduct a scientific research of a case study based on an organisation which had a substantial information leakage.
5. Conduct an interview of information security experts concerning information security practices.

Figure 2 Scientific research outline



Structure. Master thesis will consist of five main chapters. The first chapter will analyse definitions for information security management systems (frameworks), risk and incident management and E-business. Second chapter will analyse the theoretical aspects of information security including analysis used in scientific books and scientific journals, web material, analyses international standards and best practices (frameworks) for information security management. The third chapter is presenting the methodology by which the scientific research will be done. The fourth chapter is analysing a case study of the NSA which encountered an information leakage (WikiLeaks) – this case study will show that pure information security management may have huge implications even for a governmental enterprise as NSA. Fifth chapter will present the interview of information security management experts. This chapter is the main chapter for researching the issues of lack of information security management.

Keywords

Information security management, information assurance, e-business, ITIL, ISO 27000, ISO 27001, incident management, WikiLeaks, NSA, case study.

1. DEFINITIONS OF INFORMATION SECURITY AND E-BUSINESS

1.1 Information security management

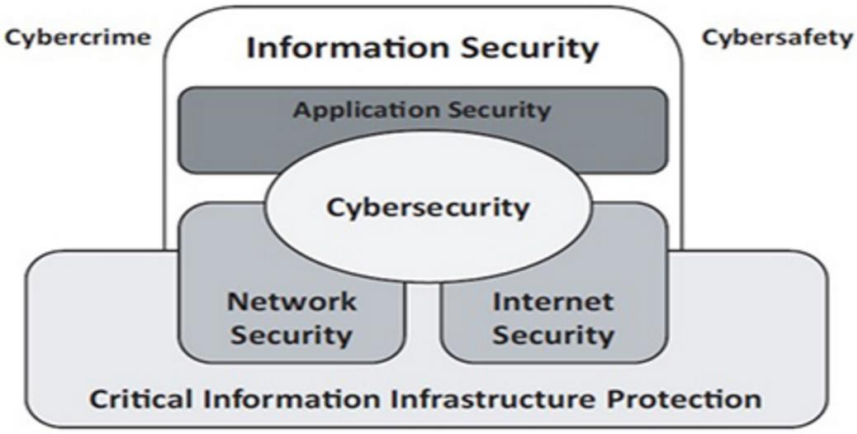
In order to do the research it is important to define what information security is about and how it has to be interpreted? Most definitions of information security used in modern information security business tend to focus, sometimes exclusively, on specific usages and, or, particular media: e.g., "protect electronic data from unauthorized use" or "keep classified information secret". In fact it is a common misconception, or misunderstanding, that information security is the same as computer security or IT security. The U.S. National Information Systems Security Glossary defines Information systems security as "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats" *[49, p. 30]*. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities *[32, p. 4]*. Information security is achieved by implementing a suitable set of technical controls, including personnel policies, security processes, information management procedures, organizational structures with information and access management included. All mentioned controls have to be established, implemented, constantly monitored, reviewed and improved (continual service improvement), ensuring that all specific security and organisational objectives are fulfilled. This should be done in conjunction with other business management processes.

It is important to point out three dimensions of information security:

- confidentiality;
- integrity;
- availability *[32, p. 5]*.

Additional review of cyber security and information security terminology and their relationship have to be conducted. Von Solms & van Niekerk are noting that "cybersecurity and information security are two distinct fields of study that nonetheless are often conflated" *[61, p. 12]*. Generally, von Solms & van Niekerk note that "Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cybersecurity, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace" *[61, p. 101]*.

Figure 3 Relationship between information security and other security domains



Source: ISACA title: Cyberspace challenge [15]

Based on the terminology reviewed we can conclude that the main difference in the nature of information security to cyber security is that information security is concentrated on the protection of the actual information in general (technical controls, including personnel policies, security processes, information management procedures, organizational structures), when cyber security deals with technical implementation how security has to be dealt with, and what is reachable through the technical infrastructure (which is not only information). This topic points the importance of general view on information security and not narrowing it down only to cyber security, it is important when planning and implementing a successful information security management model in e-business. In further research author will concentrate on information security in general and cyber security as one of the processes in achieving information security.

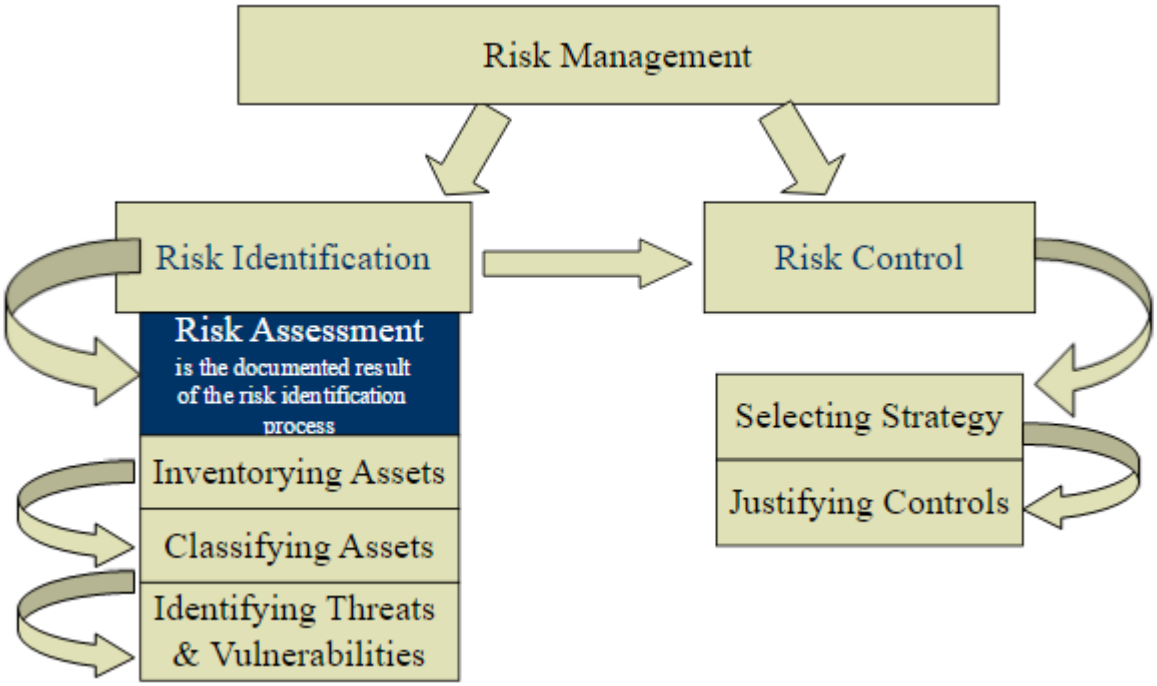
1.2 Information security risk management

Managing risks in any environment is one the most important aspects for a company of any size or business model. This action should be appropriate and proportionate the companies' level of ambition to the risk they are ready to take forward. As Alan Colder defines the risk as the combination of the probability of an event and its consequences while the risk control is defined as "means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature" *[14, p. 21]*.

Risk management is complex process which may involve all levels of management, while deployment of risk management control measures must be appropriate to risks that the business is facing. John R. Vacca is stressing that organizations interested in implementing a comprehensive security management system should start by documenting all business processes that are critical to an organization and then analysing the risks associated with them, then implement the controls that can protect those processes from external and internal threats *[60, p. 259]*.

Risk management requires two major undertakings: risk identification and risk control. Risk identification is the process of examining and documenting the security posture of an organization's information technology and the risks it faces. The second major undertaking, risk control, is the process of applying controls to reduce the risks to an organization's data and information systems *[63, p. 17]*.

Figure 4 Risk management



Source: Michael E. Whitman and Herbert J. Mattord title: Principles of information security [63, p. 17]

Business standards implement a more structural and formal information risk assessment view based on the best practices available.

The risk assessment should:

a) identify threats and their sources;

b) identify existing and planned controls;

c) identify vulnerabilities that can be exploited by threats, to cause harm to assets or to the organization;

d) identify the consequences that losses of confidentiality, integrity, availability, non-repudiation, and other security requirements may have on the assets;

e) assess the business impact that might result from anticipated or actual information security incidents;

f) assess the likelihood of the incident scenarios;

g) estimate the level of risk;

h) compare levels of risk against risk evaluation criteria and risk acceptance criteria *[34, p. 27]*.

Information security risk management is an essential process which has to find and asses the possible threats and vulnerabilities which can happen to organization and its information. Risk management goal is to secure the assets (including information) of a business that its mission and goals would be achieved. Important is that all assessed risks would be controlled and documented. It is important to stress that an a business which does not have processes in place for risk management in general and information security in particular is very prudent and non-flexible to emerging threats. From an e-business point of view it is important that management would pay appropriate attention to risk management assessment and would implement the procedures for a quarterly or an yearly risk assessment – this would give the top level managers tools to be proactive and stop or lower the chances of any possible incidents that could influence the work of an organization.

1.3 Information security incident management

While researching information security incident management it is critical to point out what is incident management as a process and what place does it take in the organisation. To disclose the nature of incident management we will review how it is covered in a leading standard for Information technology infrastructure library (ITIL).

Incident management is the process responsible for managing the lifecycle of all incidents. Incidents may be recognized by technical staff, detected and reported by event monitoring tools, communications from users (usually via a telephone call to the service desk), or reported by third-party suppliers and partners. The purpose of incident management is to "restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained. 'Normal service operation' is defined as an operational state where services and configuration items are performing within their agreed service and operational levels" *[37, p. 73]*.

Incident management as a process also includes as one of its sub-processes information security incident management. Leading information security international standard describes security incident as a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security while information security incident management processes are for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents" *[32, p. 3]*.

As ISO 27000 standard states an incident is an interruption of services. For an e-business any interruption of services can have a negative impact on business through customer trust. One of most significant information leaks in last years occurred to SONY in 2014. The information lost was so significant that SONY in a week from when the memory leak lost 10% of value per share *[41]*. This

shows us that incident management both with risk management can ensure the business continuity would not be affected or lower the damage that can happen.

For e-business to achieve a flexible and resilient incident management process it is important to apply an incident management model which would address all service interruptions and security incidents in an organization.

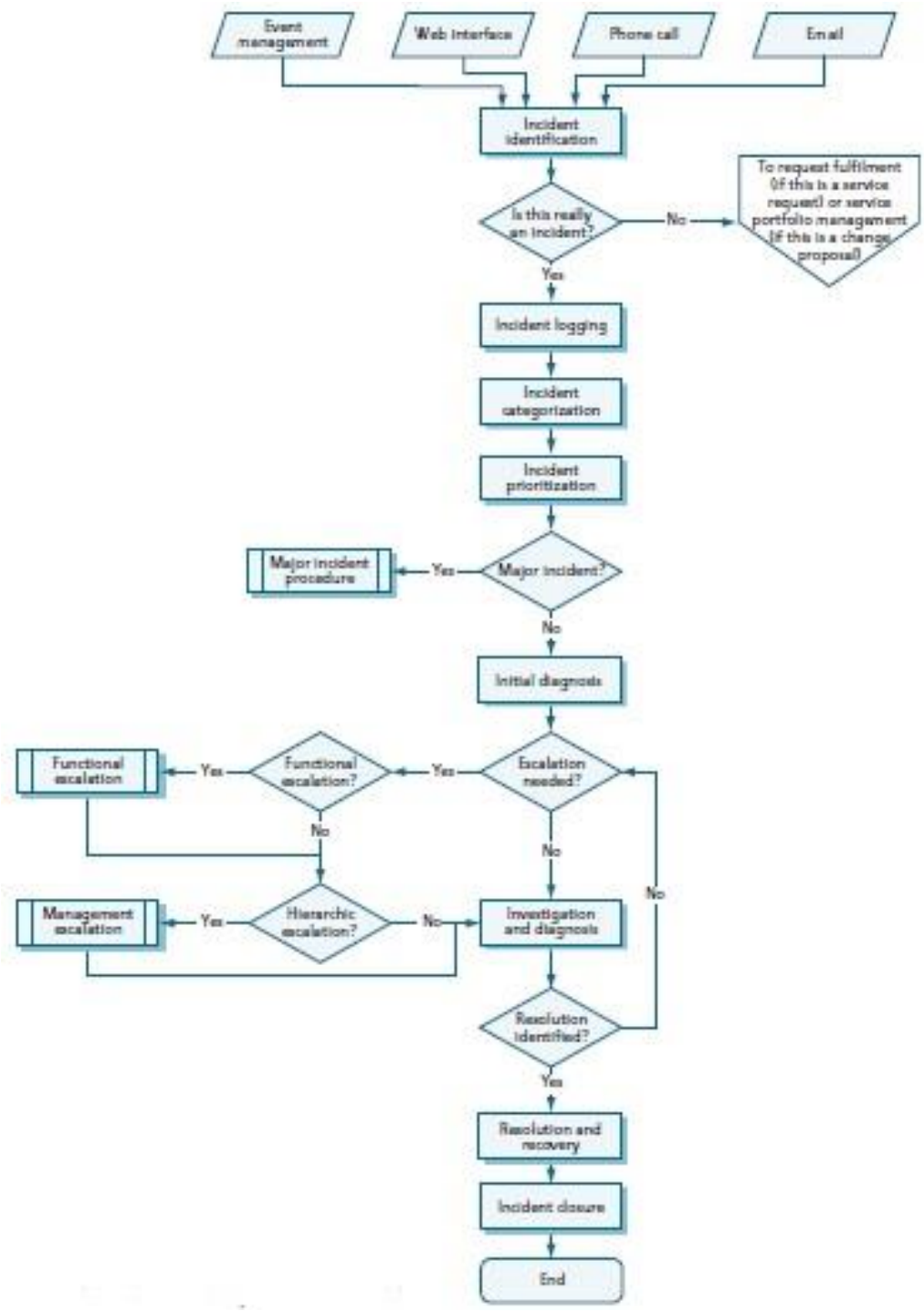
ITIL describes main points which have to be included in incident management model:

- the steps that should be taken to manage the incident;
- the chronological order incident management steps should carried out;
- responsibilities of incident management personnel;
- precautions to be taken before resolving the incident (backing up data (logs, audit files), configuration files, legal aspects);
- timescales and thresholds for incident resolution;
- escalation procedures for incidents;
- forensic evidence preservation *[36, p. 76]*.

IBM study on data leakages points out the importance of incident management form the financial perspective "incident response teams decreased the cost of data breach - an incident response team reduced the cost of data breach by $16 per record, from $158 to $142" *[1, p 2]*.

After analysis of incident management importance in information security author would like to stress that incident management is one of the key processes for creating a secure e-business environment. Incident management should work in close relationship with risk management and be prepared for any possible risks identified (information leakage, physical disruption of services). Incident management must be implemented in organization's structure and have established the main performance indicators like time to resolve an incident, incident prioritizing, forensic procedures. E-business without incident management capabilities will be more likely to have financial and reputational losses than an e-business which implemented an incident management process in their organization. Incident management practices studied are based only for service interruptions while they do not concentrate on information or network breaches and other security incidents. It crucial for e-business to implement incident management in such a way that procedures would include leakages of classified information and any other vulnerabilities. Author will in detail review the importance of incident management in the case study analysis and the interview of IT experts.

Figure 5 Incident management process flow



Source: ITIL® Service Operation title: Best management practices publishing [37, p. 77]

1.4 E-business

Based on Eurostat statistics 67 % of individuals aged 16-74 in the EU used the internet on average daily or almost daily in 2015 *[68]*. Making the e-market one of the biggest market places in EU.

While E-business is about digitally enabled commercial transactions between and among organizations and individuals. For the most part, this means transactions that occur over the internet (World Wide Web). E-business technology permits commercial transactions to cross cultural and national boundaries far more conveniently and cost effectively that is true in traditional commerce *[42, p. 297]*.

The term e-business is defined as the use of electronic means to conduct an organisation's business internally or externally. Internal e-business activities include the linking of an organisation's employees with each other through an intranet to improve information sharing, facilitate knowledge dissemination and support management reporting. Important part of e-business is supporting after sales service activities and collaborating with business partners *[17, p. 4]*.

E-business is depicting business which are carrying out their activity in an online environment. Dave Chaffey in his book E-business and E-commerce Management: Strategy, Implementation and Practice describes as "e-business is the exchange of information electronically mediated in the organization and external stakeholders to support business processes" *[17, p. 32]*.

While analysing the scope of e-business it is important to understand the whole aspect of the studied portion of it. It is important to stress that E-business includes electronic commerce and mobile commerce as a subset. *[17, p.5]*.

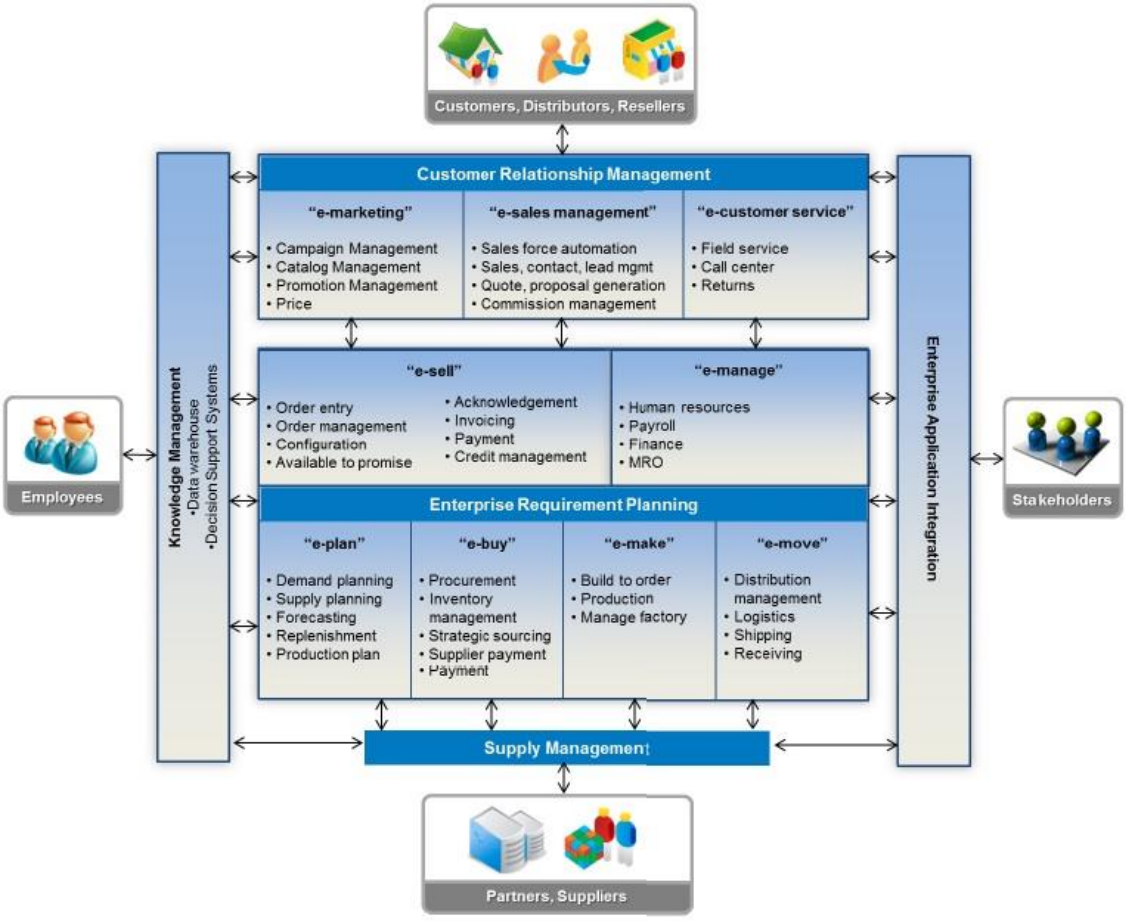
But in today's environment e-business grew and is cannot be expressed only by e-commerce and m-commerce and there multiple fields where electronic operations are gaining ground.

E-business will be interpreted in a more detailed manner including main points which are imbedded in e- business:

- e-marketing (campaign management, catalogue management, promotion management, price formation management, social media marketing);
- e-sales management (sales force automation, sales information management, quote and proposal generation, commission management);
- e-customer service (field service, call centre, returns, social media support);
- e-sell (order entry and further management, invoicing, payment management, credit management);
- e-manage (human resources, payroll, finance);
- e-plan (demand and supply planning, forecasting, replenishment, forecasting production plans);
- e-buy (procurement, inventory management, strategic sourcing, supplier payment);
- e-make (build to order, factory management);
- e-logistics (distribution management, logistics management, shipping/receiving management);

- e-commerce (business to business and business to customer service provision) *[16, p. 5]*.

Figure 6 e-business application framework



Source: Ceroni Jose, Moghaddam Mohsen, Nof Y. Shimon, Jeong Wootae title: Revolutionizing Collaboration Through E-work, E-business, And E-service [16, p. 5]

Analysing e-business scope in modern environment where there is a huge amount of different e-services that both support and drive the e-business it is impossible to distinguish one and main field of information security strategy for an e-business. E-business should be viewed as structure which is providing its service by electronic means and protects its information in electronic environment. Frequently while analysing information security for e-business there is an inaccuracy being conducted that the created information security management model is appropriate for the business at that specific moment, but is not flexible and adaptive (this limited point of view can be very inadequate in long term perspective). Author in his research will pay attention to generalize e-business and recommend an information security model which would be flexible and easily adaptable to ever changing architecture of e-business.

2. INFORMATION SECURITY MANAGEMENT

In this section of the research there will be stressed the importance of information security for an e-business from the management point of view while having in mind the need of the customer for a safe environment while conducting operations in electronic environment. Main points of this section will be to explore information security frameworks and explore best practices for security management in e-business company. Based on scientific literature there will be presented main points that security management in e-business is built from.

2.1 Information security management models for e-business

Security is an expansive term and it is difficult to narrow it to e-business just as security of the infrastructure or the office. To understand how to safeguard commercially sensitive information from competitors or subjects whom are interested to use this information against the company itself, it is critical to point out and research the whole complexity of security implementation in business as whole.

Information security is critical to ensure business continuity in the modern world. E-business managers must understand the importance of having information security processes in place because this is critical to their service provision and financial results. Based on IBM's annual study "2016 Cost of Data Breach Study: Global Analysis" it is worth to notice that from 2013 until 2016 there is a 29% increase in total cost of data breach since and the average cost per lost or stolen record is $158 *[1, p. 1]*. Business reputation is also one of key factors which influence a business after a data breach. Based on an interview conducted by IBM "51% of companies in "2016 Cost of Data Breach Study: Impact of Business Continuity Management" study said their reputation or brand had been negatively impacted because of a data breach" *[2, p. 3]*.

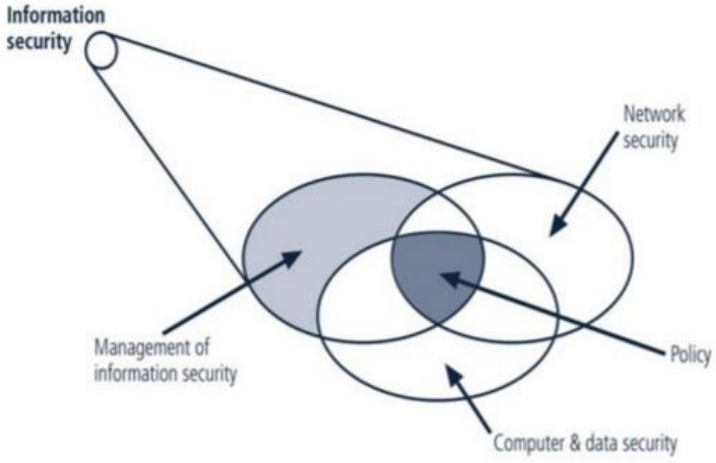
Michael E. Whitman and Herbert J. Mattord stress the simplicity of security and the complexity to be secure as "the quality or state of being secure – to be free of danger." In other words, protection against adversaries – from those who do harm, intentionally or otherwise – is the objective *[63, p. 8]*.

Following the principles of information security it is important to stress the classical six dimensions of security:

1. physical security, to protect physical items, objects, or areas from unauthorized access and misuse;
2. personal security, to protect the individual or group of individuals who are authorized to access the organization and its operations;
3. operations security, to protect the details of a particular operation or series of activities;

4. communications security, to protect communications media, technology, and content;
5. network security, to protect networking components, connections, and contents;
6. information security, to protect information assets *[63, p. 8]*.

Figure 7 Components of information security



Source: Michael E. Whitman and Herbert J. Mattord title: Principles of information security [63, p. 9]

While analysing the classical six steps of security it is important to understand the complexity of IT today and there is a need of a new way of thinking and interpreting security. To define what is security in the modern world and how it has to be looked from e-business point of view author will present Certified Information Systems Security Professional's (CISSP) used information security domains.

CISSP security domains are as following:

1. **Security and Risk Management** domain addresses the framework and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets and to assess the effectiveness of that protection;
2. **Asset Security** domain contains the concepts, principles, structures, and standards used to monitor and secure assets and those controls used to enforce various levels of confidentiality, integrity, and availability;
3. **Security Engineering** domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those control used to enforce various levels of confidentiality, integrity, and availability;
4. **Communication and Network Security** domain encompasses the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media;

5. **Identity and Access Management** domain - access controls encompass all operational levels of an organization (Facilities, support Systems, information systems, personnel identity and access management);
6. **Security Assessment and Testing** domain covers a broad range of ongoing and point-of-time based testing methods used to determine vulnerabilities and associated risk;
7. **Security Operations** domain is used to identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of critical information;
8. **Software Development Security** domain requires a security professional to asses software security and guide its hardening *[28, p. 15]*.

Considering the complexity of security implementation in organization and providing a secure environment for the customer in e-business, information security must be managed in a manner similar to any other major system implemented in an organization *[63, p. 20]*. Information security processes implementation in e-business can be done through methodological and structured sequence. One of the assessment methodologies for any type of organization is the system development lifecycle (SDLC). Principles of information security describes SDLC as a methodology for the design and implementation of an information system in an organization. A methodology is a formal approach to solving a problem based on a structured sequence of procedures *[63, p. 20]*.

Traditional SDLC consists of six general phases:

1. Investigation.
2. Analysis.
3. Logical design.
4. Physical design.
5. Implementation.
6. Maintenance and change *[63, p. 20]*.

Implementing SDLC is crucial to achieve security by design state, when a system (being it application or e-business tool) is created in such a way that security was one of the keen points in the creation process.

OWASPA methodology presents main security by design principles which are being presented below:

1. Minimize attack surface area - every feature that is added adds a certain amount of risk to the overall end state. The aim for secure development is to reduce the overall risk by reducing the attack surface area;

2. Establish secure defaults - there are many ways to deliver an “out of the box” experience for users. However, by default, the experience should be secure, and it should be up to the user to reduce their security – if they are allowed;

3. Principle of Least privilege - the principle of least privilege recommends that accounts have the least amount of privilege required to perform their business processes;

4. Principle of Defence in depth - the principle of defence in depth suggests that where one control would be reasonable, more controls that approach risks in different fashions are better. Controls, when used in depth, can make severe vulnerabilities extraordinarily difficult to exploit and thus unlikely to occur;

5. Fail securely - applications regularly fail to process transactions for many reasons. How they fail can determine if an application is secure or not;

6. Don't trust services - many organizations utilize the processing capabilities of third party partners, who more than likely have differing security policies and posture than you;

7. Separation of duties - a key fraud control is separation of duties;

8. Avoid security by obscurity - security through obscurity is a weak security control, and nearly always fails when it is the only control;

9. Keep security simple - attack surface area and simplicity go hand in hand;

10. Fix security issues correctly - once a security issue has been identified, it is important to develop a test for it, and to understand the root cause of the issue *[57]*.

A security model is the essential foundation for an effective and comprehensive security program. A good security model should be a high-level, brief, formalized statement of the security practices that management expects employees and other stakeholders to follow. A security policy should be concise and easy to understand so that everyone can follow the guidance set forth in it *[44, p. 107]*.

All security models are based on principal security blocks which are presented in figure 7, but it is important to include those models and frameworks in the research that are most reliable and respected worldwide and tuned to secure an e-business type of environment. Author for the study will present only those models and frameworks which are leaders for 2015 in information security management. Based on Gartner's quadrant for Security Awareness Computer-Based Training 2015 leaders author will present SANS institute framework on information security management as the leader for security awareness company in 2015 *[55]*. Based on IT Skills and Certifications Pay Index™ (ITSCPI) which is published annually by Foote Partners author will present ISACA's Information security manager's framework for implementations of information security processes in an organization *[30]*. Analysing the leading service management framework author will present ITIL (ISO 20000) as the service management system (SMS) standard *[31]*.

Analysing the above presented information security models it is important to stress that all best practices (frameworks) or traditional security models which were reviewed are oriented for narrow standard type of business and with emphasis on theoretical aspects. For e-business managers can be difficult to process a huge amount of information and make a decision which information

security model to follow. Based on sophistication and importance of the problem, there is a need of connecting the best practices and providing a simplified guidance based on both theoretical knowledge on practical expertise as a part of the information security model. It is also important to stress the need of SDLC when planning and creating new systems (or upgrading already existing ones) and implement through SDLC security by design. A common issue when the system is being created "as-if" and security measures are being conducted after the creation of the system (lack of strategic information security management implementation).

2.2 Information security strategy for e-business

E-business while working in cyber environment which changes at incredible speeds has to be driven to changes and flexible.

ITIL as a service management framework recognizes security management as an integral part of service management. A service strategy specifically defines how a service provider will use services to achieve the business outcomes of its customers, thereby enabling the service provider (whether internal or external) to meet its objectives *[38, p. 35]*.

To understand the essence of strategy and how information security has to be incorporated into e-business strategic plans author will present Mintzberg's introduced four forms of strategy that should be present whenever a strategy is defined:

1. **perspective** - describes the vision and direction of the organization. A strategic perspective articulates what the business of the organization is, how it interacts with the customer and how its services or products will be provided. A perspective cements a service provider's distinctiveness in the minds of the employees and customers;
2. **positions** - describe how the service provider intends to compete against other service providers in the market. The position refers to the attributes and capabilities that the service provider has that sets them apart from their competitors. Positions could be based on value or low cost, specialized services or providing an inclusive range of services, knowledge of a customer environment or industry variables;
3. **plans** - describe how the service provider will transition from their current situation to their desired situation. Plans describe the activities that the service provider will need to take to be able to achieve their perspective and positions;
4. **patterns** - describe the ongoing, repeatable actions that a service provider will have to perform in order to continue to meet its strategic objectives *[38, p. 39]*.

E-business environment has to deal with challenges which have to be implemented in all four forms of strategy with emphasis on information security strategy. In the primary stages of e-business strategy planning, information security strategic planning has to be implemented to carry out all the

processes needed to ensure information security. Based on ISO 27000 it's stressed that "within the overall strategy and business objectives of the organization, its size and geographical spread, information security requirements can be identified through an understanding of:

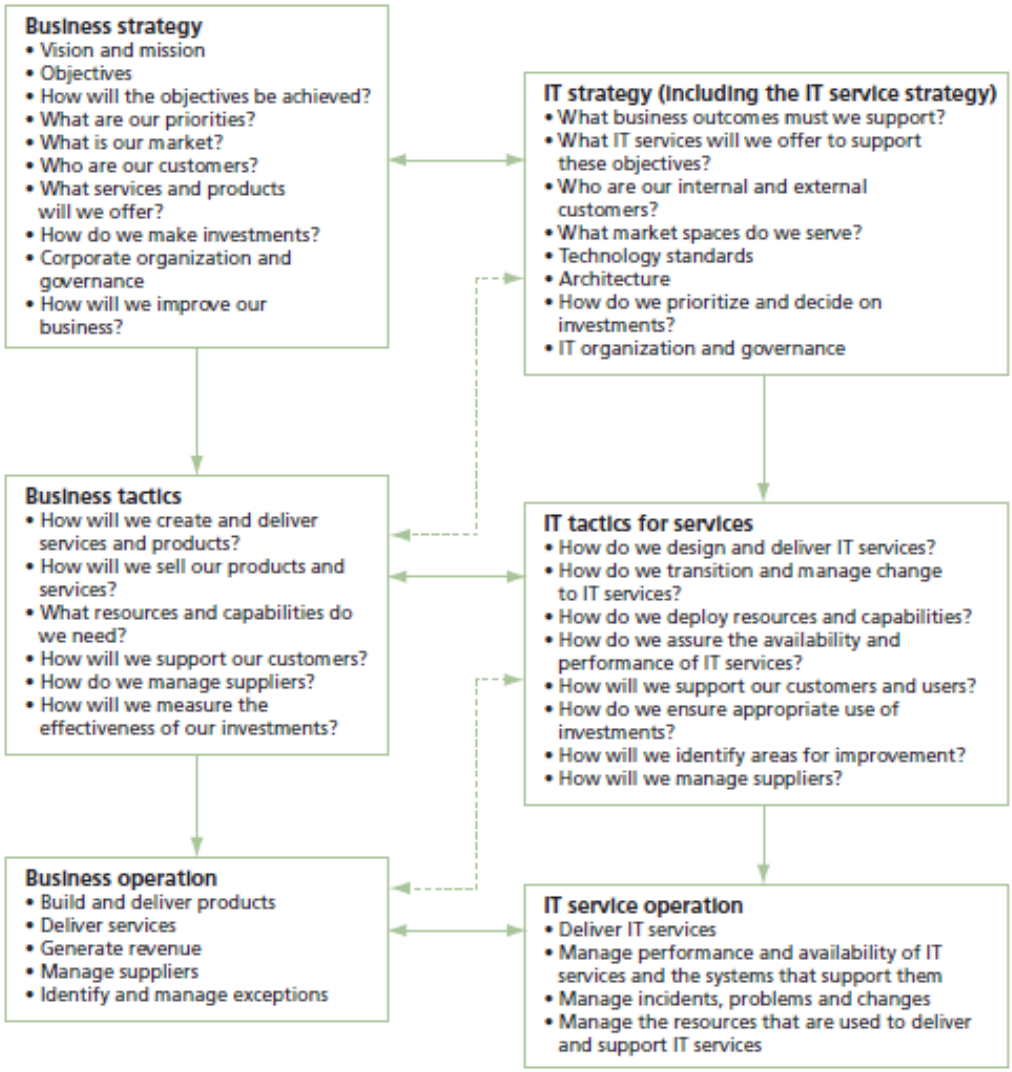
a) identified information assets and their value;

b) business needs for information processing and storage;

c) legal, regulatory, and contractual requirements" *[32, p. 10]*.

IT operations are derived from the IT tactics, but also by the requirements of business operations. The way in which the different operational environments are coordinated and how they interact is very important for strategy management for IT services. It is only once a strategy has been executed, that it can be validated. Assessment of the actual performance of activities and services can indicate whether the parameters used in setting the strategy were accurate, and can also validate any assumptions made *[38, p. 136]*.

Figure 8 The scope of strategy management



Source: ITIL® Service strategy title: Best management practices [38, p. 135]

There multiple solutions to evaluate the policy of a company concerning information security and what steps have to be made that this policy would comply with market standards.

Laura Lewis in article concerning information security “Cyber Center: Practical Strategies for Developing a Cyber-Incident Plan” presents an two step plan which information has to be gathered and what has to be implemented to ensure an entry level of information which has to be taken into account when creating an information security strategy.

First, using its own resources or that of a contractor, a company should inventory the information and types of data in its possession and the information it is collecting in the normal course of business across all departments. Next, the location and methods for accessing this information should be identified and documented. For better planning, the company's data should be categorized using a five-point ranking system:

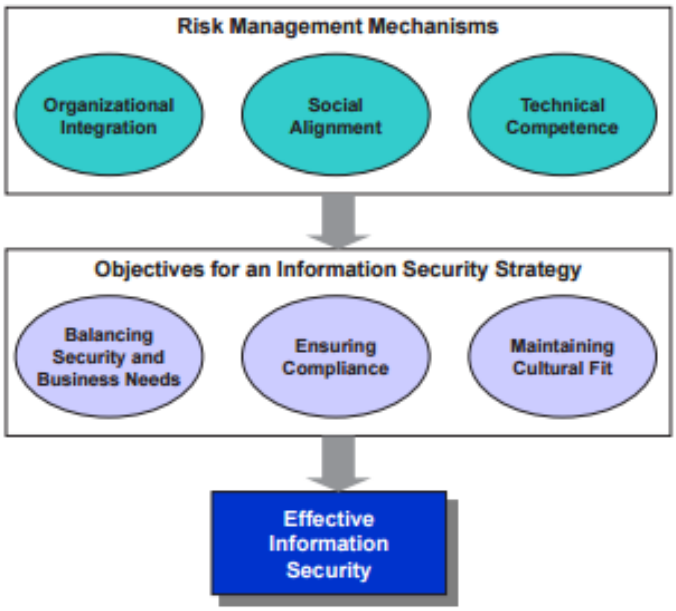
1. critical to key business operations;
2. sensitive personally identifiable information;
3. important to management and operation;
4. peripheral maintenance and historical information;
5. significant and redundant information *[43, p. 5]*.

Laura Lewis stresses the need to store the data in a safe manner that it could not be intercepted and modified. Strategic requirements for data storage would follow:

1. confirm the system has a firewall;
2. routinely use encryption and protect the encryption key by storing it outside the server;
3. routinely install security patches, software updates, and malware protection;
4. mandate that passwords include complex character combinations and expire every 60 to 90 days without allowing an employee to reuse them;
5. structure, implement, and enforce bring-your-device policies;
6. consider mobile device management (MDM) software for monitoring, managing, securing, and wiping mobile devices remotely;
7. evaluate the use of cloud computing or limit the types of data approved for cloud use, and never provide the encryption key to the cloud provider *[43, p. 4]*.

There are three primary objectives all security executives must address regardless of the organizational context: balancing the need to secure information assets against the need to enable the business, ensuring compliance, and maintaining cultural fit. Achieving these objectives will ensure the security function is strategically focused, business driven, and aligned with the organization. Of particular interest is the strategy used to accomplish these objectives and achieved it through a socio-technical strategy that includes three types of critical risk management mechanisms: organizational integration, social alignment, and technical competence *[40, p. 163]*.

Figure 9 A Strategic Framework for Effective Information Security



Source: Kayworth, T., & Whitten, D. title: Strategic Framework for Effective Information Security [40, p. 163-175]

E-business has to follow a strategy to achieve effective information security in the organization. Methodologies presented show how a strategy has to be created and what has to be reviewed before the strategy acceptance, but do not emphasize strategic thinking for information security. E-business environment because of its complexity and need for flexibility has to adopt strategic thinking for information security in such a way that it would be flexible to changes and include all critical process while operation (risk management, incident management, information security models). Creation of an e-business information security strategy has to balance the security with business needs, working environment friendliness and customer conception of the e-business. It is important to view information security in a general view and not to narrow the strategy of the company only to a formalized document which presents guidance for specific process (often forgetting information security), but more as a link of all the processes in the organization. Strategies presented do not provide critical guidance on aspects like incident management when ITIL and other sources are stressing the importance of this processes in the organization. At further research author will stress the unification best practices and standards to distinguish a flexible information security model.

2.3 Information security architecture for e-business

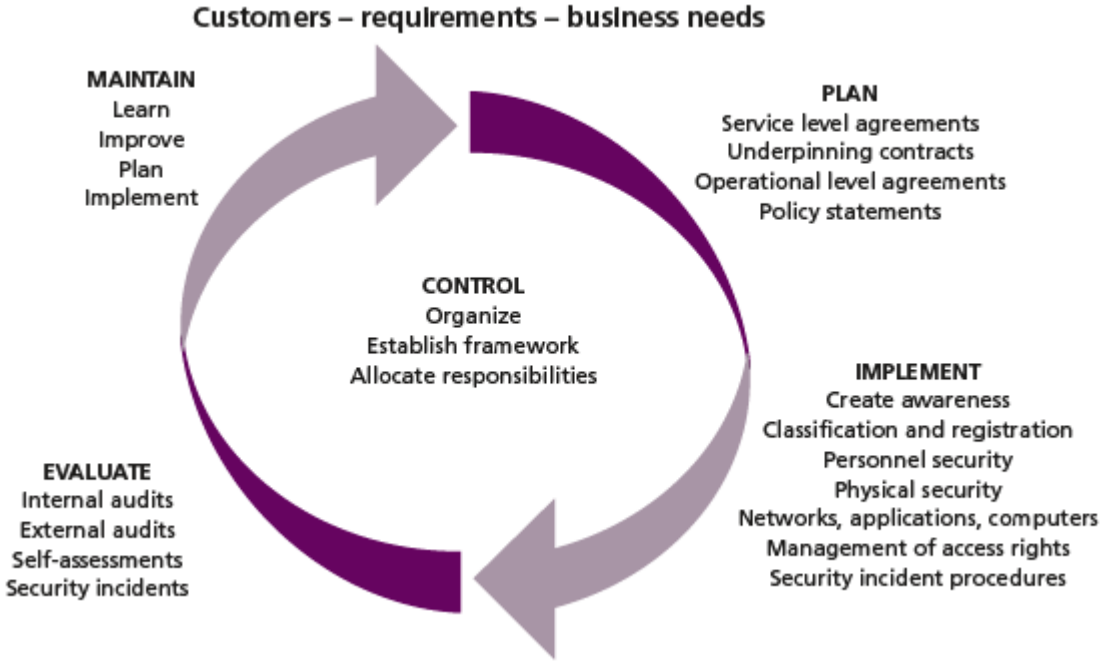
E-business is different from a classic type of business. This enforces the e-business management to concentrate on fields of operation that do not occur in the classic businesses and the most difficult in e-business organization is the architecture of information security roles. In this

section author will briefly present main guidelines for a holistic information security architecture for e-business.

ITIL framework points out that the "objective of information security architecture management is to protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity and availability" *[36, p. 197]*.

Based on ISO/IEC 27001 formal standard which businesses tend to obtain an independent certification of their information security management system (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the business) *[36, p. 99]*.

Figure 10 Basic architecture of an information security management system



Source: ITIL® Service design title: Best management practices [36, p. 99]

While creating an e-business information security infrastructure it is important to follow simple and non-complex frameworks. As Jason J. Burkett suggests "SABSA methodology is an enabler of business, providing features and advantages that lead to many benefits for every layer of an organization, regardless of the existing enterprise architecture *[12, p. 53]*.

The SABSA methodology consists of six layers from which each of them is representing the view of a different layers of management personnel in the enterprise *[12, p. 49]*.

As a methodology SABSA consists of six layers which are mapped to six stakeholder views, and the six interrogatives defined for each layer of a business security architecture. SABSA methodology takes a holistic approach in identifying security solutions for business problems that executives face, not the "technically led approach" that solves only the tactical operational issues, this

is important and helps to analyse the organizational structure of e-business and evaluate the implementation of information security assurance methods *[12, p. 49]*.

FIGURE 11 The SABSA® Matrix for security architecture

LAYERS	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)	VIEWS
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization & Relationships	Business Geography	Business Time Dependencies	Business
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies & Architectural Layering	Security Entity Model & Trust Framework	Security Domain Model	Security-Related Lifetimes & Deadlines	Architect
Logical	Business Information Model	Security Policies	Security Services	Entity Schema & Privilege Profiles	Security Domain Definitions & Associations	Security Processing Cycle	Designer
Physical	Business Data Model	Security Rules, Practices, & Procedures	Security Mechanisms	Users, Applications, & the User Interface	Platform & Network Infrastructure	Control Structure Execution	Builder
Component	Detailed Data Structures	Security Standards	Security Products & Tools	Identities, Functions, Actions, & ACLs	Processes, Nodes, Addresses, & Protocols	Security Step Timing & Sequencing	Tradesman
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management & Support	Application, User Management, & Support	Security of Sites, Networks, & Platforms	Security Operations Schedule	Service Manager

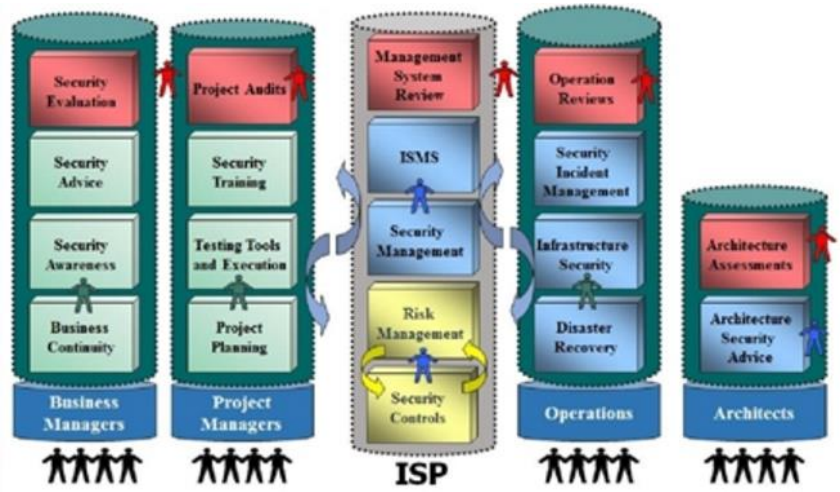
Source: Burkett, J. S. title: Business Security Architecture [12, p. 49]

SABSA methodology is very important when the information security architecture has to be defined through the layers of the personnel conducting the security management roles and different views in organization, but it does not emphasize the distribution level between management staff and technical staff. John Frisken in his review of information security program in comparison to COBIT presents the importance of personnel division into managerial and technical staff to achieve different goals of business management *[25, p. 3]*. SABSA methodology is a minority in comparance with other methodologies, but its stresses one of the important aspects in information security and that is the importance of viewing the problem from functions or people point of view, but it does not offer a way how to combine managerial and technical staff.

Basic methodologies include a multipoint overview on security and multi-layered approach to understanding the security measures that have to be achieved. One of multipoint architecture methodologies that will be presented is Trust Information Security Architecture or TISA. Based on basic principles how business information security architecture has to be build and presented by the author up to this section, it is important to finalize the main principles of the information security architecture. Robson de Oliveira Albuquerque and Luis Javier García Villalba are researching TISA and offering a non-comprehensive tactics to achieve this architecture - a way to assess security is

based on a layered architecture with components connected in such a way that everything is part of a puzzle that must be connected, so information security should be seen as a complex figure in whole business management *[6, p. 5]*.

Figure 12 Leveraging COBIT to Implement Information Security



Source: Frisken, J. title: Leveraging COBIT to Implement Information Security [25, p. 3]

More detailed presentation of TISA architecture will done based on a publication "A Layered Trust Information Security Architecture" by de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati and Tai-Hoon published in Sensors journal in 2014 *[6, p. 6]*.

1. **Layer 1:**

Layer 1 of TISA methodology consists of sub items that have to be addressed.

1.1.Data, Information, Information Systems, Information Assets, Networks.

This is the layer in which data is important to organizations or in which individuals are found or mapped. Stressing the importance of data to any type of business nowadays, information can be retrieved from data and information systems. Reviewing information assets, it is also very important that they are audited and properly labelled, and the relationship to information should be clearly understood by the organization and the personnel responsible for its protection.

1.2.Confidentiality.

Confidentiality is one of the most important aspects of information security and it is responsible to prevent unauthorized access to information. Main principle of confidentiality is "need-to-know", and in order to be effective, confidentiality must ensure that access to critical information is given only to authorised personnel.

1.3.Availability.

Information has a specific value or use depending on a specific task which has to be carried out and when it has to be carried out (information must be available when necessary). To acquire information, all information systems, networks, databases, information assets, must be accessible by the authorized personnel. If information is unavailable (lost or destroyed) or the access for authorised personnel was delayed or denied the availability of information is insufficient.

1.4.Integrity.

Integrity is a guarantee that the data is accurate and consistent trough transmission and the whole lifecycle. Considering information a valuable asset, data or information should not be unauthorizedly (or secretly) deleted or modified, which would affect the information. Integrity has include the possibility to check whether data was modified or not and to determine all actions executed to the data.

1.5.Information Security Extensions.

Information security has to be interpreted as special extensions of group of new attributes or properties intended to protect information and systems, but that are not limited to it.

It is possible to stress the main extensions as following:

- authentication;
- access control;
- non-repudiation;
- authenticity;
- privacy;
- anonymity;
- authorization.

Extensions are defining information security from a more detailed perspective *[6, p. 6-7]*.

2. Layer 2:

Layer 2 of the architecture will present which technologies and by which personnel should be used and how all of this information should be provided to higher level management.

The following items will disclose all points of layer 2:

2.1.Information Security Policy.

The information security policy is a high-level document that provides essential requirements and procedures that should be followed in the sphere of information security. This policy document is very specific (while centring on information security) and covers only one organization (branch). The information security policy also determines procedures like security incident management and information security controls. Information security policy should be implemented in such a way that it would be tuned to organisational needs and operational environment.

2.2. Processes.

Information security policy processes provide formal mechanisms which identify, measure, manage and control risks related to information. Processes are critical when an incident accurse and evidence should be gathered, thus it should formalised and implemented in an organisation and followed thoroughly.

2.3. Personnel.

"Personnel" is the number one subtopic of the architecture methodology and represents human resources management. It is important to understand that employees create and manage security processes in the organisation at any given time. When planning information security policy, it is critical to address points concerning personnel security, such as strategy related to hiring new employees, dismissal, responsibilities, damage caused to information, access to information, training, and whatever is critical to achieve business success and maintain organisations information security strategy.

2.4.Technology.

Technological aspects of information security are changing in great speed, they are becoming obsolete while being the core of the organisations infrastructure. Technologies one of the most important aspects is to lower the risks of possible information security incidents and provide new ways of securing information. Technology should be viewed as one of integral parts of information security, but not the main one.

3. Layer 3:

This layer represents processes that deal with daily activities and how they should be done.

3.1.Normatives and Procedures.

Basically, a normative document with procedures emphasizes what and when has to be done (which processes) when dealing with important information. Normatives are critical for an organisation to prioritize main goals, plan and organize all processes handled in information security.

3.2.Auditing.

Audit asses all points of information security including information assets, data storage assets, procedures and documentation.

3.3.Continuous Monitoring.

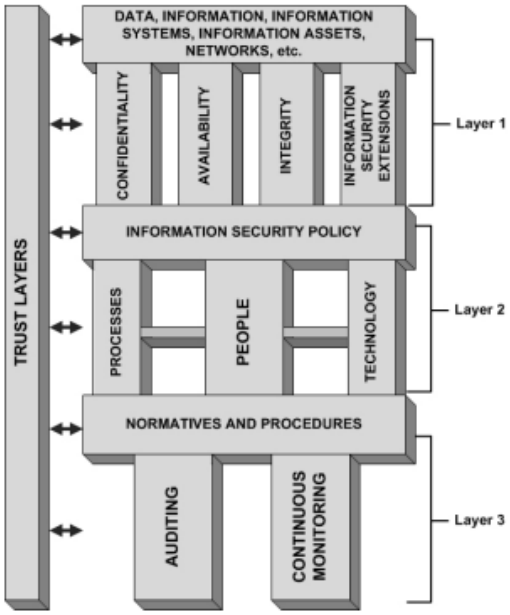
Continuous monitoring tracks of all knowledge on information security including known vulnerabilities and possible threats. This information is critical for risk management that proper assessment would done.

4. Trust Layer:

Trust is a believe that all processes will work as intended and it can be measured by empiric research and observation, and by the evaluation of the IT systems and the processes implemented in the organisation. Trust may be established if all of the expectations were achieved in all layers of the company's information security management. From an information security management point of view to trust something or somebody all aspects of the processes involved should be identified and work as planned. It also must not do anything it was not supposed to do and must be able to operate nonstop. Trust and information security management are related. Security objectives are considered, it is clear that trust is connected to security, because information security depends on people and

security extensions, such as authentication, authorization, access control, non- repudiation *[6, p. 6-7]*.

Figure 13 TISA: Layered trust information security architecture



Source: de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati, F., & Tai-Hoon, K. title: A Layered Trust Information Security Architecture [6, p. 6]

Analysing information security architectures which should be implemented for e-business we can notice that the main offered frameworks are not e-business driven, but more driven to a classic type of e-businesses. Either one of the methodologies are stressing the importance of technical and both technical/managerial personnel in information security architecture, but are stressing different points which have to be achieved. Often managers without proper technical background are leading technical decisions without understanding their real implications for implementation or maintenance – this practice may lead to an enlarged budget for IT maintenance or result in a critical vulnerability in the infrastructure. Author will be stressing the importance of technical knowledge in e-business information security management.

2.4 Information security processes for e-business

Information security plays a key role in XXI century business. Analysing information security from an e-business perspective it is important to mention that information security is an integral part of service management. To research and present main processes that should be included in service management the author will use ITIL framework. Although ITIL is not a security management process establishing framework, but it is important because ITIL is based on best practices and the framework includes information security management as a part of service management *[44, p.239]*.

ITIL from a service design point of view considers that service security processes include:

1. A policy;
2. An Information Security Management System **(**ISMS**);**
3. Structure and controls;
4. Risk Management;
5. Communication strategy *[36, p. 85]*.

Information security as whole is a decision made on a strategic level which implementation has to be done in the design phase of the creation of organization processes, and in a situation when it is not implemented then it has to be done in service transition phase of company evolution. Rebuilding and reconstructing the organizations processes to reach the level of ambition to have a secure environment can be demanding and resource consuming *[39, p. 67]*.

To compare main similarities and differences between and industry standards author will also present leading industry standards for information security. ISO 27001 standards which describes information technology, security techniques, information security management systems and requirements is the leading information security industry standard which is being implemented also in governmental sector. Main points of ISO 27001 would be:

1. Control;
2. Plan;
3. Implement;
4. Evaluate;
5. Maintain *[33, p. 2-6]*.

ISO 27001 standard emphasizes the importance of leadership in security management in organization. Strategic way ahead for information security will influence the design of information security processes. ISO 27001 demonstrates the "steps which have to be concluded by the top management personnel to achieve a sustainable design for information security processes:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement;

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility" *[33, p. 2]*.

Processes as whole are mainly based on best practices. Based on a research published in the Journal of Enterprise Information Management by Abhishek Narain Singh M.P. and Gupta Amitabh Ojha there was presented a summary of best practices which should be implemented:

1. regular updates of anti-virus software to safeguard systems against virus/malware processes;
2. proper authentication for external connections;
3. reviewing information security incidents;
4. submitting reports to higher management;
5. asset management;
6. access control to IT systems and services;
7. information security incident management plan;
8. access log tracking *[58, p. 660]*.

Because researched information security architectures are mainly focused on security implementation and not on the operation of e-businesses in an electronic environment. Author will use ITIL service design roadmap in order to develop an effective and efficient service solutions guidance for creation of processes that meet security standards for e-business conducting their economic activity in cyber environment, it is critical that the inputs and needs of all other areas and processes included in the service design are considered and reviewed within each of the service design activities *[36, p. 85]*.

ITIL as framework provides critical processes that have to be implemented in an e-business. Author will present the critical processes that have to be implemented in an organization to achieve a coherent level of service management and information security management:

1. incident management – the most important process in a company. Used to manage high priority service interruptions including security incidents. The process is owned by an incident manager;
2. problem management – important process which is critical in long term perspective. Establishes the root cause of an occurring incident and proposes a permanent fix for the service being investigated. The process is owned by an problem manager;
3. release and deployment management – the process is intended to review new software and evaluate its influence to the whole architecture of an organization. Process is critical in information security management from the point when new security being implemented. The process is owned by release and deployment manager;
4. change management – process which based on information and procedures gathered by other processes permits or denies a change in environment. ITIL best practice uses Change advisory boards to cooperate with other process owners. The process is owned by change manager;

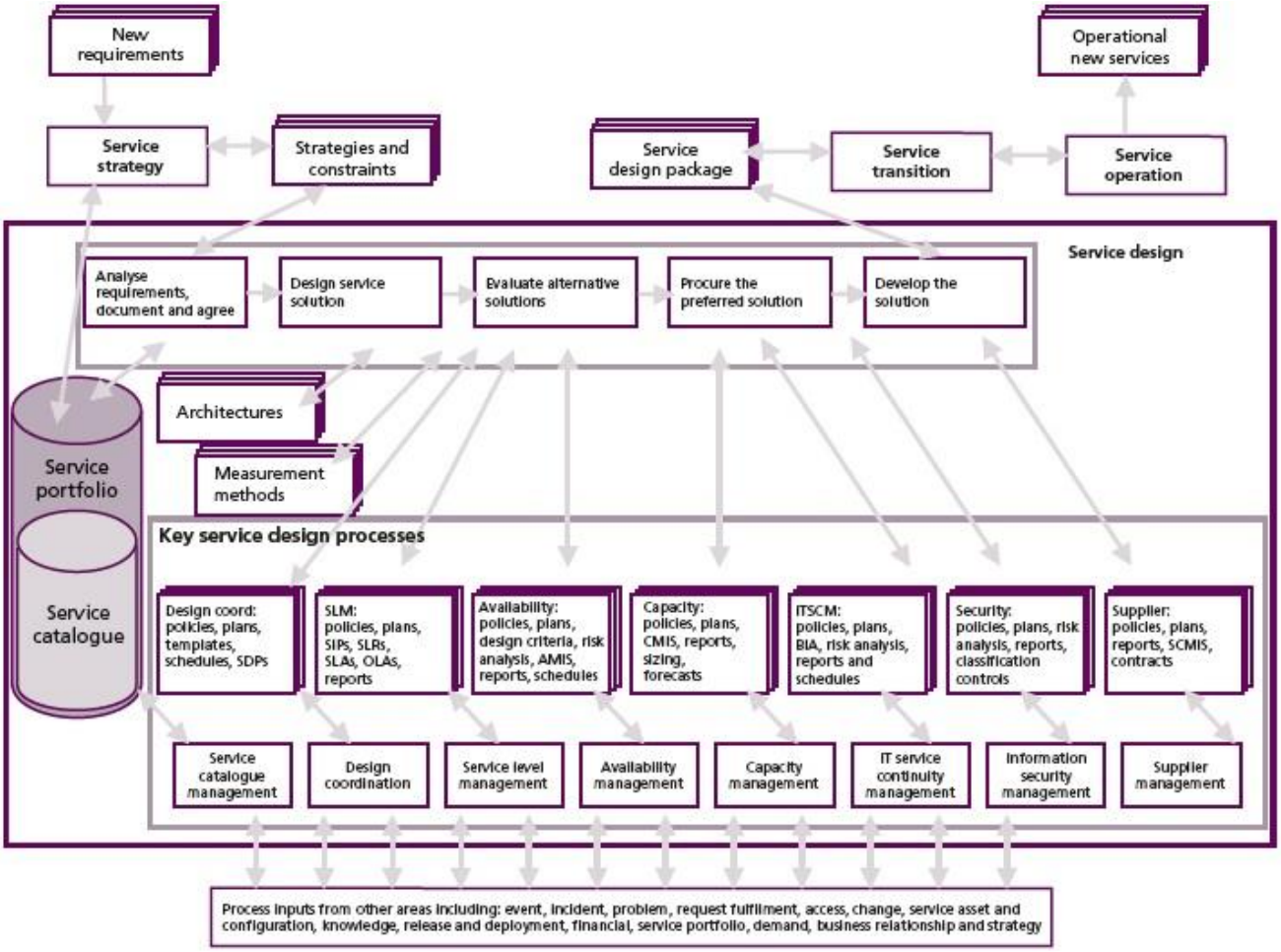
5. service asset and configuration management – process which ensures that all stakeholders which own or use the data and relationships for the service architecture are meeting with the level of integrity required. The process is owned by configuration manager;
6. service level management - acts as the single point of service management and ensures that the service portfolio and service catalogue meet the requirements indicated in service or operational level agreements. The process is owned by the service manager;
7. availability management and capacity management – technical team responsible for the monitoring of system availability and the resources needed to meet the requirements. The process is owned by the availability/capacity manager;
8. IT service continuity management – process is responsible to restore the system in a situation of crisis (audits the technical part of the infrastructure recovery systems). The process is owned by the service continuity manager;
9. information security management – the process intended to control other processes to that they would meet the information security policy. The process is owned by the information security manager/officer (INFOSEC);
10. financial management for IT services – process intended to monitor the quality of IT infrastructure to the price and the return of crisis management (time to restore a service) *[36, p. 258-265]*.

To manage processes ITIL as framework is offering to distinguish process owners for each process or group of processes. Process owner role is accountable for ensuring that a process is usable (fit for purpose) as it was intended in the design phase. Best practice is that this role would be assigned to the personnel who carries out the process manager role for the processes in his area of responsibility (also while analysing larger organizations - the two roles may be separate). The process owner (manager) role is accountable for ensuring that the process they are accountable for is performed according to the agreed and documented standards and meets the goals of the process definition *[36, p. 259-260]*.

Basic responsibility (which the process owner is accountable for) of the process owner is:

- sponsoring, designing and supporting the change management process and its key performance metrics;
- defining the process strategy;
- ensuring that appropriate process documentation is available and current to the standards which have to be met;
- ensuring that process technical staff have the required knowledge and the required technical skills and also business understanding to deliver the process both to the customer and to the organization, and understand their role in the process;
- reviewing opportunities for process enhancements and for improving the efficiency and effectiveness of the process *[36, p.259-260]*.

Figure 14 Service design – the detailed picture



Source: ITIL® Service design title: Best management practices [36, p. 85]

All researched topics and methodologies until this point of master thesis have revealed the steps which have to be done to secure the information in an organization. It is important to note that the standards and methodologies show what has to be done (asset audit, information classification, management of different systems), but mainly emphasizing the technical procedures to be implemented either nonspecific actions to be taken (which are more oriented to a classic type of business). On the other hand ITIL is providing a firm explanation of processes and their need in the organization, but is not a security driven framework. While e-business environment depends in huge matter to availability of the services and this points out the need of incident management, availability management, change management and other ITIL framework processes. Author points the misconception between security driven standards and methodologies (being based only on security measures and not paying enough attention to quality service provision) and service provision frameworks (which concentrate on service provision and not on the security operations) – this incompatibility leads to a programmed conflict when following only security driven standards and methodologies will create paranoic and user unfriendly environments while the service provision framework will lead to user friendly service provision but with low concentration on security. The goal is to achieve a model for system security implementation in e-business which would unite both

the need for security and service provision standards in such a way that it would not affect neither of them.

3. RESEARCH METHODOLOGY FOR THE RESEARCH

Author to research the topic will use qualitative research methodology based on a case study and an interview of information security experts. This chapter will present the method and the design of the research conducted.

Denzin and Lincoln interpret a qualitative research as "situated activity that locates the observer in the world. Qualitative research consists of a set of interpretative, material practices that make the world visible. These practices transform the world. They turn the world visible. They turn the world into a series of representations, including field notes, interviews, conversations, photographs, recordings and memos to self. At this level qualitative research involves an interpretive, naturalistic approach to the world. This means that qualitative researchers study things in their natural settings, attempting to make sense of, or to interpret, phenomena in terms of the meanings people bring to them" *[21, p. 9]*.

Peter Swanborn describes a case study research as "study carried out within the boundaries of one social system (the case), or within the boundaries of a few social systems (the cases), such as people, organisations, groups, individuals, local communities or nations-states, in which the phenomenon to be studied enrols" *[59, p. 13]*.

Robert Yin points out that "doing a case study research remains one of the most challenging of all social science endeavours." *[67, p. 3]*. Also it is important to understand that a case study was picked as the research method by the author because of the nature of the problem being investigated. Author will try to answer how the situation in the case researched happened and why did it happen, while focusing on contemporary events.

The interview will be carried out in person or by sending an online interview form.

3.1. Model for scientific empirical research methodology

The research process performed by the author in this thesis is based on a method proposed by Robert Yin of a single case study *[67, p. 51]*.

Robert Yin notes that a single case study has numerous advantages "The single case study is an appropriate design under several circumstances, and five single-case rationales – that is, having a critical, unusual, common, revelatory, or longitudinal cases." *[67, p. 51]*.

Research will be carried out trough combining Robert Yin's 5 phases of conducting a case study *[67, p. 3-6]* and 6 stages which are noted by Donald R. Cooper and Pamela S. Schindler in Business research methods *[19, p. 74]*.

Robert Yin 5 phases	Donald R. Cooper and Pamela S. Schindler 6 stages	Scope of the research concluded by the author
Plan	Stage 1: Clarifying the Research Question	• Review of scientific literature • Identification of a research problem
Design	Stage 2: Proposing Research	• Identification and development of an appropriate research strategy • Single CASE study selection
	Stage 3: Designing the Research Project	• Identification of an appropriate research method • Development of a research protocol • Document research method identification
Prepare	Stage 4: Data Collection and Preparation	• Interview of information security experts • Collection and organization of documents
Collect		
Analyse	Stage 5: Data Analysis and Interpretation	• Analyse and discuss information from the CASE study and interpretation using existing theory and best practices
	Stage 6: Reporting the Results	• Empirical conclusions and interpretations

3.1.1 Stage 1: Clarifying the Research Question

John Gerring in Case study research: principles and practices stresses the importance of understanding the purpose of the research "it is impossible to pose questions of research design until one has at least a general idea of what one's research question is. There is no such thing as case

selection or case analysis in the abstract. A research design must have a purpose, and that purpose is defined by the interference that it is intended to demonstrate or prove *[26, p. 71]*.

Stage I of the research process starts with the authors development of an understanding of the relevant problem or societal issue being studied. This process involves working with the academic community to refine and revise study questions to make sure that the questions can be addressed given the research conditions (time frame, resources and context) and can provide important and trustworthy information *[10, p.4]*.

Leonard Bickmanm and Debra J. Rog in the Applied social research methods handbooks notes that at the first stage of the research there have to be 3 main points addressed:

1. Understand the problem;
2. Identify questions;
3. Refine/revise questions *[10, p. 5]*.

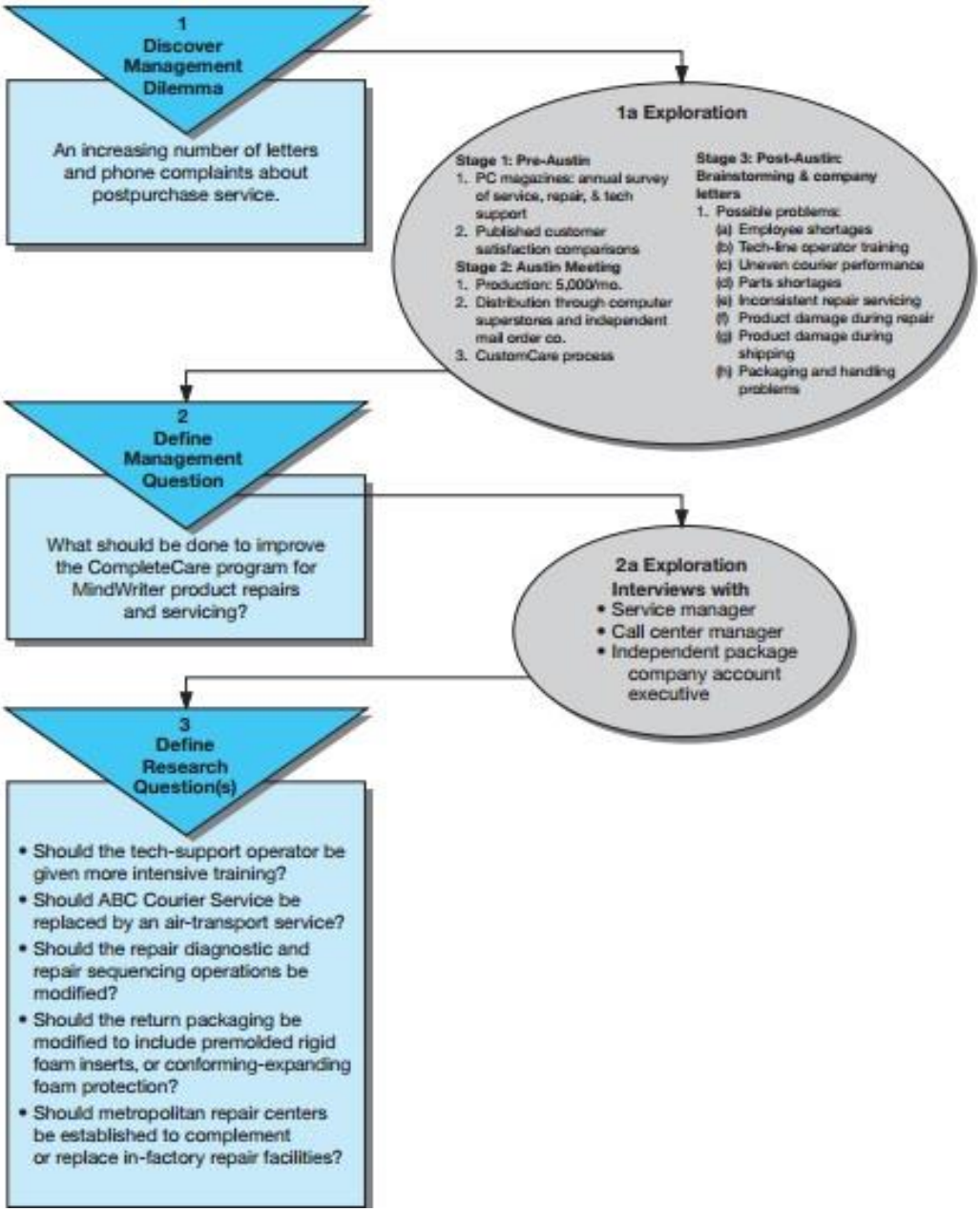
Understanding the problem is the milestone for a successful research. To find a source for the problem author has to pick the problem from 4 main areas:

1. problems that are suggested or assigned by an advisor or mentor;
2. problems derived from technical and nontechnical literature;
3. problems derived from personal and professional experience;
4. problems that emerge from the research itself *[20, p. 21]*.

Robert Yin also stresses the importance of research question and proposes guideline how find the problem of the research "defining the research questions is probably the most important step to be taken in a research study, so you should be patient and allow sufficient time for this task. The key is to understand that your research questions have both substance – for example, what is my study about? – and form – for example, an I asking a "who", "what", "where", "why", or "how" question?" *[65, p. 10]*.

Donald R. Cooper and Pamela S. Schindler in Business research methods suggests that "a useful way to approach the research process is to state the basic dilemma that prompts the research and then try to develop other questions by progressively breaking down the original question into more specific ones. The outcome of this process is the management–research question hierarchy." *[19, p. 77]*.

Figure 15 Formulating the research question



Source: Cooper R. Donald, Schindler S. Pamela title: Business research methods [19, p. 78]

3.1.2 Stage 2: Proposing Research

After clarification of the research question and proposing a research (finalizing the research questions) it is worth to understand the nature theory of the problem that will be researched. John Gerring claims that "theories are tested when they are pushed to their limits, when they are tried out in very different contexts. Root Bernstein observes that this strategy leads, at the very least, to an investigation of the boundaries of an idea, a useful thing to know. Alternatively, it may help us to reformulate a theory in ways that allow it to travel more successfully, that is, to increase its breadth. A third possibility, perhaps the most exciting, is that it may lead to a new theory that explains the new empirical realm *[27, p. 49]*.

The research question is the central question which the researcher in his research intends to answer. The research problem has to be focused in a sufficient manner and properly defined in order to formulate clear and understandable research questions. It is critical to formulate a clear research question, because it directs the whole research project (through all of the stages of the research). Gathering right data for the search is heavily dependent on clear and relevant research questions – consequently this provides the right data and answers to the research questions and a successful research in a whole *[11, p. 24]*.

Robert Yin notes that one of the steps which should be taken before proposing a research topic is conducting a selective or a comprehensive review of literature *[66, p.62-63]*.

In this stage of the research author will stress the need of Robert Yin's proposed comprehensive literature review as the most suiting to propose a research question.

"Turning to the topic of comprehensive literature reviews, there are occasions when such reviews are warranted. The reviews aim to bring together what is known on a particular topic, possibly highlighting controversial or disparate line of thinking or even the progress over time in cumulating knowledge about a subject. The legitimate role of this type of review is indeed recognized by the existence of major journals, in nearly every social science discipline and subject area, devoted exclusively to such literature reviews." *[66, p. 63]*.

3.1.3 Stage 3: Designing the Research Project

The research design is the milestone to pursue the objectives and answer the research questions. Selecting an appropriate research design may be complicated by the availability of a large variety of different research methods, protocols, procedures, techniques and sampling plans.

After identifying a research question it is important to plant the further steps of the research project. It is important to decide which methodology will be used for the research.

Martin Davies and Nathan Hughes the two principal options that can be chosen as following:

1. "You can choose quantitative research methods, using the traditions of science.
2. You can choose qualitative research, employing a more reflective or exploratory approach." *[24, p. 23]*.

Pertti Alasuutari in his article The Globalization of qualitative research, published in qualitative research practice describes "doing a qualitative research as a very data-driven process in the sense that most of the time one has to proceed inductively from empirical observations towards more general ideas regarding theory or methodology. When proving that our interpretation is valid, suggesting an interpretation, or weighing the pros and cons of different interpretations, we also typically give examples or take excerpts from the qualitative data, for instance from transcribed interviews or from video recorded naturally occurring situations." *[5, p. 595]*.

Robert Yin describes the design as "the logical sequence that connects the empirical data to a study's initial research questions and ultimately, to its conclusions." *[67, p. 28]*.

A case study research has to have 5 components which are especially important:

1. case study questions;
2. case study propositions (if any);
3. case study units of analysis;
4. the logic linking the data to the propositions;
5. the criteria for interpretation of findings *[67, p. 29]*.

Robert Yin stresses the importance using analytic generalization in single case study researches. Robert Yin emphasizes that "analytic generalization may be based on either corroborating, modifying, rejecting, or otherwise advancing theoretical concepts that are referenced in designing the case study or new concepts that arose upon the completion of the case study. The important point is that, regardless of whether the generalization was derived from the conditions specified at the outset or uncovered at the conclusion of the case study, the generalization will be at a conceptual level higher than that of the specific case." *[67, p. 41]*.

3.1.4 Stage 4: Data Collection and Preparation

Data collection is one of the main tasks which have to be concluded in a logical way to answer the research questions. Data can be defined as "the facts presented to the researcher from the study's environment. First, data may be further characterized by their abstractness, verifiability, elusiveness, and closeness to the phenomenon." *[19, p. 85]*.

Preparation for data collection should have:

1. desired skills and values;
2. training;
3. developed protocol for the study;
4. interview questions;
5. pilot case study *[67, p. 71]*.

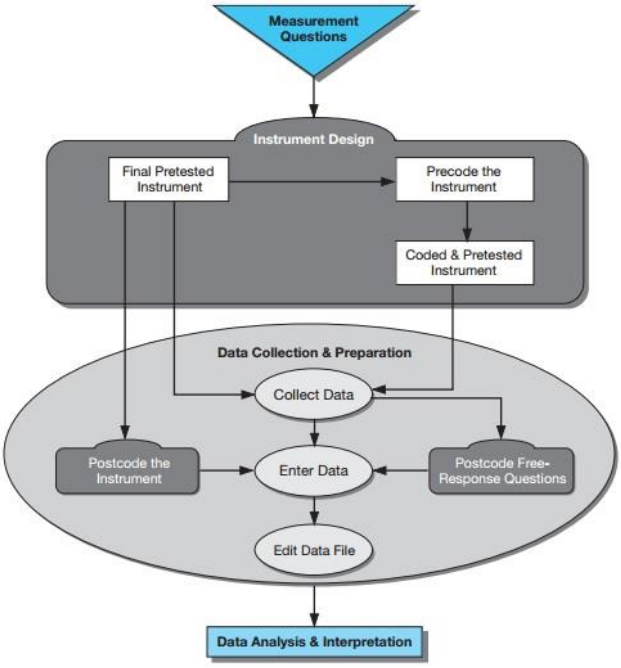
Author in his research will follow data collection methodology based on five out of six sources of evidence *[67, p. 106-109]*.

Source of evidence	Strengths	Weaknesses	Used in this research
Documentation	- stable – can be reviewed repeatedly; - unobtrusive – not created as a result of the case study;	- Retrievability – can be difficult to find; - biased selectivity, if collection is incomplete;	Reviewed numerous documentation to corroborate and augment evidence from other researched sources.

	- specific – can contain the exact names, references, and details of an event; - broad – can cover a long span of time, many events, and many settings.	- reporting bias – reflects (unknown); - access – may be deliberately withheld.	
Archival records	- Same as those for the documentation; - precise and usually quantitative.	- Same as those for the documentation; - accessibility due to privacy reasons.	Reviewed: - Risk report; - Audit report; - Organization change report; - Yearly report; - Organizational records.
Interviews	- Targeted – focuses directly on case study topics; - insightful – provides explanations as well as personal views; - questioner – provide a more objective way to interview the targeted audience.	- Bias due to poorly articulated questions; - response bias; - inaccuracies due to poor recall; - reflexivity – interviewee gives what interviewer wants to hear.	Reviewed: - Interview of information security experts from international enterprise level businesses.
Direct observations	- Immediacy – covers actions in real time; - contextual – can cover the case's context.	- Time-consuming; - selectivity – broad coverage difficult without a team of observers; - reflexivity – actions may proceed differently because they are being observed - cost - hours needed by human observers.	Used articles and information from workers and other personnel whom was related with the organization studied.
Participant-observation	- Same as the above for direct observations; - insightful into interpersonal behaviour and motives.	- Same as the above for direct observations; - bias due to participant-observer's manipulation of events.	This method was not used to gather information in this study due to geographical restrictions.
Physical artefacts	- Insightful into cultural features; - insightful into technical operations.	- Selectivity; - availability.	This method was not used to gather information in this study due to geographical restrictions.

Managing data and preparing it for analysis is a critical success factor that have to be achieved. Donald R. Cooper and Pamela S. Schindler present data preparation that it "includes editing, coding, and data entry and is the activity that ensures the accuracy of the data and their conversion from raw form to reduced and classified forms that are more appropriate for analysis. Preparing a descriptive statistical summary is another preliminary step leading to an understanding of the collected data. It is during this step that data entry errors may be revealed and corrected." *[19, p. 376]*.

Figure 16 Data Preparation in the Research Process



Source: Cooper R. Donald, Schindler S. Pamela title: Business research methods [19, p. 376]

3.1.5 Stage 5: Data Analysis and Interpretation

Analysing data there should be two criteria's stressed – reliability (precision) and validity *[27, p. 159]*.

John Gerring defines this criteria's as following:

Precision – "usually understood as reliability in measurement contexts – refers to level of stochastic (random) error, or noise, encountered in the attempt to operationalize a concept and validity refers to systematic measurement error, error that by definition – introduces bias into the resulting concept (and presumably into any causal analysis that builds on that concept)" *[27, p. 159]*.

In a qualitative research data analysis process usually involves reducing big amounts of data to a manageable and more understandable size, creating summaries, examining patterns, and using statistical techniques *[19, p. 86]*.

Scientific literature stresses four general strategies while analysing data:

1. relying on theoretical propositions;
2. working your data from the "ground up";
3. developing a case description;
4. examining plausible rival explanations *[67, p. 136-140]*.

Also author will use four out of five analytic techniques as described by Robert Yon in Case study research.

Overview of the four analytical techniques *[67, p. 136-140]*:

Analytic technique	Short summary
1. Pattern matching	Compares an empirically based pattern (that is), to one based on findings from the case study.
2. Explanation building	Main point is to analyse the case study data by building an explanation about the case.
3. Time-series analysis	In time series, there may only be a single dependent on independent variable.
4. Logic models	Stipulates and operationalizes a complex chain of occurrences or events over an extended period of time.

3.1.6 Stage 6: Reporting the Results

As a general rule the reporting stage of research is one of the most demanding and sophisticated. Author after the research of a single case study and the interview of information security experts will be done, will present the results of the research as in a theory building structure.

4. A CASE STUDY

Author will analyse and present a single case study which was a major classified information breach. The case will be the NSA breach of security which had major classified information leakage. The case will not study an e-business enterprise but governmental type of organisation (NSA) to evaluate practices of security management in an enterprise level organisation which can afford to hire best security personnel and implement most advanced technologies in information security assurance. The result of the case will be the analysed procedures of security management and their comparison to best practices and interviewed security expert's opinions.

4.1. Background for the case

The case study analysed is about 2010 November 28th security incident when several thousand classified documents have been published on a website called WikiLeaks. This classified information leakage brought major information security investigations on possible classified information breaches in all governmental organisations worldwide. One of the key points investigated in the beginning of the leakage was the person's position who could steal the information. Second point considered was under what circumstances classified documents could be leaked (downloaded or copied and taken out). It is also important to stress that from the security point of view, government data networks (and, as such, belonging to the armed forces or NSA) usually are properly supervised by highly specialized and trusted specialists defending the network from cyber threats. However, military and intelligence networks are deployed in different areas around the world, and they are managed (including security issues) locally. The management of the network when locally-based, had major bandwidth limitations

(no more than 1 Mbps). All of this points showed that the NSA leakage of information could happen in a variety of places worldwide and that a cyber-attack could have taken place *[48, p. 14]*.

4.2. Presentation of the case enterprise

To understand the essence and main goals of NSA it is important to review their mission "The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances *[47]*. As we can see main mission of the NSA is SIGINT and IA while working in the environment of CNO. This important to review, because if NSA is not a e-business type of an organization from the private sector point of view it still a "provide of service to the US government" in computer network operations.

While analysing the organizational chart of NSA it is important to note that NSA have never disclosed any official organizational charts, but to analyse their structure we will investigate their structure before 2010 leaks occurred and after the period mentioned. The NSA is led by the Director of the National Security Agency, who serves as Chief of the Central Security Service and Commander of the United States Cyber Command and is the highest-ranking military official of all of these organizations. He is assisted by a Deputy Director, who is the highest-ranking civilian within the NSA. NSA also has an Inspector General, head of the Office of the Inspector General (OIG), a General Counsel, head of the Office of the General Counsel and a Director of Compliance, who is head of the Office of the Director of Compliance *[47]*.

From declassified documents we can see that NSA as of the mid-1990 was organized into five Directorates:

1. **The Operations Directorate**, which was responsible for SIGINT collection and processing;
2. **The Technology and Systems Directorate**, which develops new technologies for SIGINT collection and processing;
3. **The Information Systems Security Directorate**, which was responsible for NSA's communications and information security missions;
4. **The Plans, Policy and Programs Directorate**, which provided staff support and general direction for the Agency;
5. **The Support Services Directorat**e, which provided logistical and administrative support activities *[45, p. 130, 138, 156–158]*.

As we can see the directorates even without in depth review of the functions embedded do not show any service management structures except the support services directorate. To evaluate the changes that happened after the 2010 information leakages we will investigate the NSA structure as

of 2013. We will look into the presentation of NSA done by a security analyst Marc Ambinder. The structure researched and covered by Marc Ambinder "It has five operational directorates, several administrative directorates and three large operational centres. Each is headed by an associate director, and each associate director has a technical director" *[8]*.

Main NSA directorates as of 2013 are:

Foreign Affairs Directorate interacts with foreign intelligence services, counterintelligence centres;

Information Assurance Directorate is the centre of NSA's cyber warfare and defence program offices. This directorate is responsible to defend US government networks;

Signals Intelligence Directorate helps determine the requirements of the NSA customers — other agencies, the president, the military. The super-secret work of SIGINT collecting and offensive cyber warfare is the responsibility of S3, with its many bland sounding and compartmentalized branches.

Research Directorate is one of the critical directorates as they research deciphering.

Technology Directorate implements the technological architectures researched by the research directorate. This directorate is also responsible for maintaining all of the NSA's infrastructure.

NSA acquisition and procurement Directorate supports NSA in procurement;

Human resources Directorate responsible mainly for personnel security, but also for overall policy in information security *[50]*.

Author in this case study will concentrate only on the directorates of research and human resources as they one which control the information security processes in the organization analysed. This processes will be analysed in more depth further.

4.3. Information security management

The case study analysis and in particular the case study of classified information leakages from NSA should be investigated from the point of view of functions and processes. To research this topic in more depth author will research NSA Human resources directorate and its underlying subdivisions.

Human resources directorate consists of 12 subsections:

1. Office of military personnel;
2. Office of civilian personnel;
3. Human resources operations;
4. Information policy division;
5. Office of security;
6. Security policy staff;

7. Physical security division;
8. Field security division;
9. NSA classification advisory officer;
10. Security awareness;
11. Polygraph;
12. Counter intelligence *[8]*.

For further analysis we will research information policy division, office of security, security policy staff, physical security division, security awareness and polygraph divisions.

Information security policy division is responsible for standard implementation which carried out as procedures and guidelines. This created the rules how information security should be handled based on legal acts.

Office of security is the central division were information about personnel is being stored. This division mainly gathers information about people who possibly are involved in espionage or terrorism against the U.S. *[52]*.

Security policy staff is the division where staff security officers are. This division's personnel is responsible to guide military and civilian personnel trough security measure implementation in organization *[51]*.

Physical security division is responsible for physical security of infrastructure and classified areas.

Security awareness division provides security guidance and briefings regarding unofficial foreign travel, couriers, special access, temporary duty assignments, and amateur radio activities *[51]*.

Polygraph division concludes polygraph interviews for personnel management. This interview is intended to check the person's reliability to work in the organization *[54]*.

As we can see information security management from processes and functions point of view is very strict and well documented. It important to stress that NSA is about 30 000 employee big *[8]*. To manage information in an organization that big it is critical to control the risks and manage changes accordingly. It is important to note that while investigation of possible processes in NSA there were no processes found that manage incidents, service management, change management or a centralized access management – this can be seen through investigation of NSA's structure and responsibilities of different divisions (also review of all NSA's manuals which are available in open sources did not emphasize existence of any of management functions mentioned). From the review of the organizational structure we can see that the studied organization has a difficult and complex structure where each division has it dedicated role. This type of information security management is very sluggish and non-flexible. Security processes tend to become formal and inconvenient. As ITIL best practices stresses there should be processes for continual service improvement to withstand the changes in the environment. Analyses of NSA information security management structure shows that

it is a slow, non-flexible process which because of its difficulty and non-user friendliness maybe interpreted just as a formality.

4.4. IT Security management

From the point of view of e-business, the research of NSA information leaks are important because of the NSA experience in safeguarding information. NSA with huge capabilities still is losing sensitive information to the public. NSA employee's security manual states that "information may be useful only if it is kept secret" *[51]*.

As e-business and NSA operate mainly in electronic (cyber) environment it is important to research information security management from more technical security processes point of view. In this chapter author will investigate the NSA's processes for IT security management as part of information security management processes. To carry out this research author will investigate the processes in Technology directorate as it is responsible for the technical implementation and overall management of NSA infrastructure.

Technology directorate consists of:

Enterprise Systems Engineering and Architecture (TE)

1. Information and Systems Security (public key infrastructure and program management office);
2. Independent Test and Evaluation;
3. Mission Capabilities;
4. Business Capabilities;
5. Enterprise IT Services (responsible for NSA telecommunications centre, known as the Global Enterprise Command centre, responsible for transport field services and for deployable communications operations;
6. High Performance Computing;
7. Technical SIGINT & Ground Capabilities *[53]*.

Researching the functions and processes of NSA Technology directorate author will research and stress the information and systems security, enterprise IT services divisions. It is important to mention that main divisions in maintenance of infrastructure are the information and systems security which are responsible for program management and the enterprise IT services which are also responsible for deployable CIS operations. It important to manage the risk of deployable CIS operations because of the operational environment where they are working – that are operations outside of the country with very bad infrastructure and ever changing personnel whom administers those systems *[48, p. 15]*. Also researching the documents and policies created by the NSA technology directorate (documents investigated: Cable Installation at NSA Facilities and Field

generation and over-the-air distribution of COMSEC key in support of tactical operations and exercises) present the NSA's Technology directorate's position in security information management. As per documents researched it can be marked that NSA's security management policies are being done in partial division between Human resources directorate and technology directorate, when technology directorate is preparing only technical and specific procedures *[13]*.

Reviewing the IT security management in NSA it is important to mention that NSA Technology directorate which is responsible of maintenance of the infrastructure (so also for information security) does not have any divisions which would carry out service management, change management or continual service improvement functions – lack of this management cells has highly negative potential to the end state of security management in an organizations because of the complexity of the organisation. With a functional division of policy creation and technical procedure creation as in NSA it is very difficult to create flexible systems when balancing user friendliness and system security level. Without continual service improvement systems used may be effective in short term, but will be very unsuccessful in long term as the users will get unsatisfied with the systems and will not follow the policy.

4.6. Information security procedures implemented in the organization

Based on the declassified documents author will research internal policy in information security. This is important to evaluate how security risks are being managed in the organisation. For the research of this procedures author will analyse NSA document Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities *[18]*. This document is concerns both physical and technical security as stated "Technical Specification sets forth the physical and technical security specifications and best practices" *[18, p. 1]*. It is important to analyse through the points which designate how risk management is being done. The risk management process includes a critical evaluation of threats, vulnerability, and assets to determine the need and value of countermeasures.

The process of risk management should include the following:

1. **Threat Analysis**. Assess the capabilities, intentions, and opportunity of an adversary to exploit or damage assets or information;
2. **Vulnerability Analysis**. Assess the inherent susceptibility to attack of a procedure, facility, information system, equipment, or policy;
3. **Probability Analysis**. Assess the probability of an adverse action, incident, or attack occurring;

4. **Consequence Analysis**. Assess the consequences of such an action (expressed as a measure of loss, such as cost in dollars, resources, programmatic effect/mission impact, etc.) *[18, p. 2]*.

Further research carried out analysed the security in depth guideline in Information security management. The NSA guidelines stress 7 points for security in depth as follows:

1. Definition of security in an certain environment (if it is physical security, then it is a definition of the environment);
2. Requirements (formal requirements for the authorization);
3. Access Control rules;
4. Visual Protection of assets displaying classified information;
5. Closed Storage (not used assets must be locked);
6. Open Storage (if assets have to be kept in open storage, additional security measures apply like access control to the office);
7. Acoustic and Technical Security (technical security of rooms) *[18, p. 5-6]*.

From the basic security in depth points and further analysis of the documentation shows basic guidelines that are used to mitigate threats mainly from the outside. It important to stress that NSA implemented risk management and assessment system does not follow best practices from information security point of view and is based mostly on external threat sources and not on the internal (asset audit, internal risks, personnel risks). All of the analysed procedures and the whole document provide a comprehensive view on information security which is backed by strict rules and policies. Also it is important to note that majority of strict rules (like the rule storage documents when not in used) are user non friendly and may be not used by the users because of their inconvenience. This points are very important when information security strategy being established and security by design has to be implemented through all the lifecycle of all the functions and processes. Key point to stress is that the security system in whole lacks flexibility, like probability analysis – in a situation when an information leakage have never occurred the probability for an incident of this sort will be very low, so there will be no crucial measures taken to withstand this probability, but if an information leakages appear then the probability will be raised and special measures will be taken (but in fact the whole process may take a long period of time and start only after the memory theft got known).

4.7 Information security breaches

After researching NSA's structure and possible procedures author will analyse information leakages that happened directly from NSA and got public. This information is important to research the process more in depth collate them to already identified problems. To investigate the case study

we will research two known major information leakages made by Edward Snowden and US Army Pfc. Bradley Manning. All major information breaches were made public by WikiLeaks, a multi-national media organization and associated library (founded by its publisher Julian Assange in 2006). WikiLeaks specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption. It has so far published more than 10 million documents and associated analyses *[62]*.

Investigating information security leakages in NSA we will not research the stories behind the criminal acts but author will note the way how information was stolen and which processes according to the best practices had stop this theft at a procedural level and why this processes did not work in NSA's case. It is important to stress that both Snowden and Manning cases were insider attacks or insider threats – this is when an insider (person working in the company) can maliciously or unwittingly steal, erase, or expose sensitive data for a variety of reasons. At the same time, insiders must be given a certain level of access in order for a business to function or an organization to operate *[46, p. 4]*. It is also worth to notice that after many insider attacks which occurred in the last decade – this type of an attack is being assessed as one of the most high risked vulnerabilities in any type of organization *[22]*.

Both Snowden and Manning cases were based on physical theft of classified data and thus it has to be portrayed as security incident and not a cyber incident. In both cases both actors were stealing data through a long period of time and carried it out from the secured zone. It is important to stress that both Snowden and Manning presented oaths not to disclose any classified information and both of them were checked by special authorities and granted security clearances to work with classified information [45, p. 45].

Researching how such big amounts of classified data were in possession of low level employees (Snowden was an intelligence analytic and Manning was private first class) it is important to distinguish the roles of "need to know" when a higher standing official makes a decision that the person has the right get acquainted with classified information and need to share when classified information is being sent over electronic media (trough classified networks) and is not being audited or controlled in any way. From the amount of information stolen it possible to assume that neither one of the persons had a possibility to have a "need to know" basis on such an amount of documents, so they could possess them only if someone has shared them or by acquiring them in an illegal manner (stealing or illegal copying). Snowden as a contractor working for NSA had a top-secret security clearance and he was working as an administrator for NSA's system – allegedly Snowden stole majority of information through a "thin client" while administrating NSA's systems and downloaded them to a media [23].

After research of both cases it is important to note that NSA's as an organization which is dealing with classified information did not implement proper authentication management

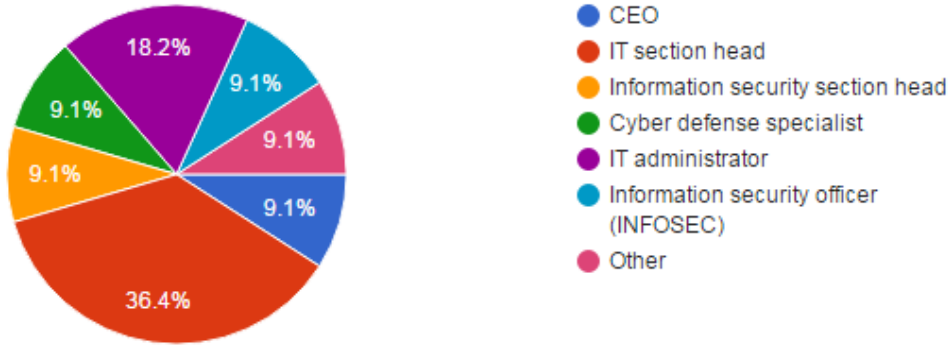
(unauthorised personnel could acquire classified information), access management (unauthorised personnel could copy and carry out classified information) and proper risk management (majority of risks were facing outside threats and the whole information security management was built on risk probability of an outside threat factor). Investigating the information thefts in general it is evident that proper access management both to information and to classified security areas was accomplished unsatisfactory and reviewing the management structure of the organization it evident that neither service management, incident management, problem management, access management functions were carried out. NSA information leakages can be evaluated from the security by design point of view when the system created (NSA information exchange networks) with a stress to achieve security, but not to evolve this security measures (lack of continuous service improvement).

5. INTERVIEW RESEARCH

The aim of this chapter is to present the data gathered by an interview of IT security experts from e-businesses. This interviews dedicated to evaluate the theoretical findings acquired by the author in the theoretical part of this research and both the case study. Author will present the characteristics of the respondents, interview findings and presents the results of the interview.

Interview based on a questioner was carried out by interviewing information security, IT security and Cyber security experts from companies which are mainly or partially e-businesses. All of the respondents at the moment of the interview were managers or heads of specialised sections/divisions working in the sphere of security management. The interview was carried out from 4th till 12 of November 2016 with 11 experts interviewed (6 face to face and 5 through a targeted electronic form that was sent to their official email box). It is important to note that because of the sensitive topic of information security management in different organizations it was agreed that neither company names either the names of persons interviewed will not be documented or mentioned in the research on purpose not to disclose any sensitive information which could miss interpret or damage the operational environment of the businesses.

Figure 17 Responders position in their organisations



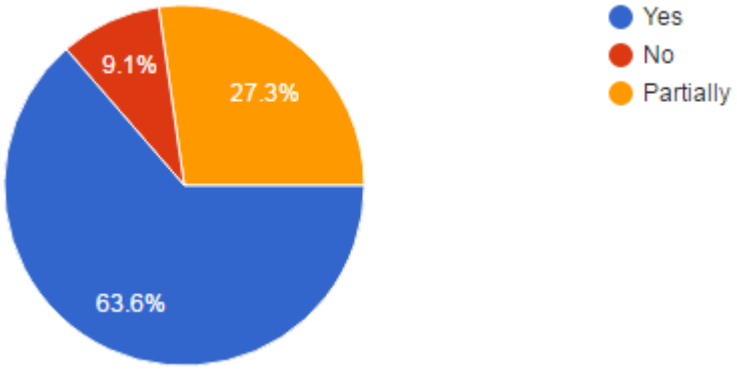
As we can see from the chart only one person answered other as their position from the main positions given in the questioner. It is important to notice that about 91% or 10 out of 11 are working in the sphere of information security and majority of them 36% or 4 out of 11 are IT sections heads in their corresponding companies.

Table 1 Amount of employees in the responder's organisation

Responder	Amount of employees
1	14000
2	130000
3	700
4	20000
5	400
6	150
7	1200
8	180
9	45
10	~2500
11	300
Total amount	169 475

As we can see from the table the whole amount of personnel working in the responders companies is 169 475 and averaging from 45 employees to 130 000 employees. With an average of 15406.8 employees per responder and a median of 700 employees per responder.

Figure 18 Responder's organisations dependence to E-business



As we can see from the chart above majority of responders organisations can be affiliated with e-business – 90,9% (10 responders) being E-business or partially E-business when only 9,1% (1 responder) being from a non E-business company.

Figure 19 Responders possession of a degree in Information Systems or Telecommunications

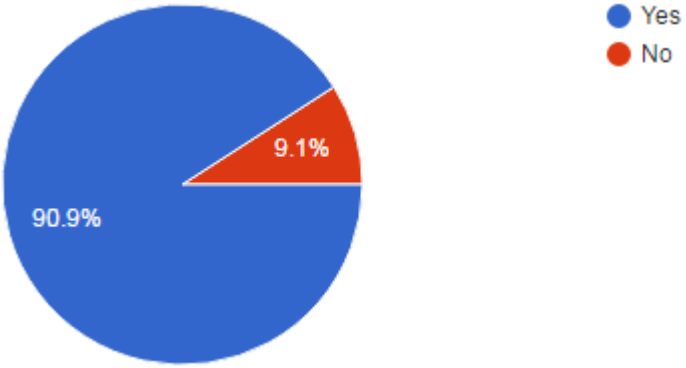
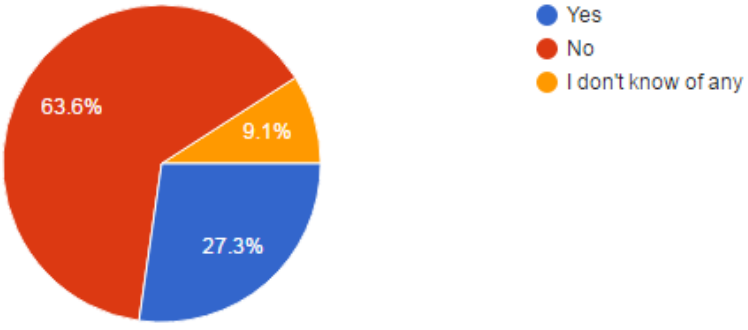


Chart above presents the degree that responders had in the moment of the interview. With a majority of responders having a degree in Information systems or telecommunications -90,9% (10 out of 11) and only 1 responder whom does not possess a degree in information systems and telecommunication 9.1%.

Concluding information about the responders in the interview it is strongly evident that the interviews were performed with experts in the field of information security (10 out of 11 are working in information security or cyber security) whom are both practically experts and with proper background education (10 out of 11 have a degree in information systems or telecommunications).

Figure 20 Information leakages which occurred in the responders organisations



As we can see from the chart above information leakages for sure occurred with 3 responders from 11 (27,3%) and with 1 responder not possessing any information about information leakages in

his organisation (9,1%). While 7 out of 11 responders answered that there were no information leakages from their companies. This chart is very important to stress that almost 27,3% of responders know of an information leakage that happened in their company.

Question No. 6 from the interview addressed the information security experts what is the main reason of information security breaches in their opinion. 100% of responders noted that the main reason in information security breaches is the human factor. Responders based on their expertise and organisational structure stressed 6 main points of human failure in information security breaches.

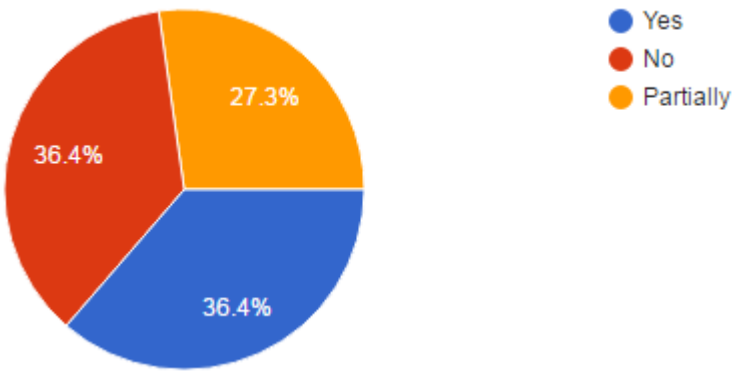
While 3 responders mentioned that their companies had information leakages it is also important to note that 100 % responders mention human factor as the main reason of information leakages.

Table 2 Responders noted information security breach reasons

Reason for the breach	Responders mentioned the reason
Personnel negligence	2
Lack of knowledge/training	3
Lack of procedure or processes or bad management	2
Employee illegal activity	3
An error caused by the technician who made the configuration of a system	1

From the points provided by the experts we can notice that all the reasons of information breaches are with involving personnel and or company employees. It is important to stress the points that are mentioned in the most cases – lack of knowledge/training and employee illegal activity, in both cases the threat is coming from the inside of the company and while personnel negligence can be also viewed as both lack of knowledge or training or as illegal activity.

Figure 21 Usage of ITIL framework in responder's organisations



After reviewing responders answer to the questions concerning the usage of ITIL best practices it is worth to mention that 63,7% of responders (7 out of 11) use ITIL in their organisations

fully – 36,4% (4 out of 11) or partially 27,3% (3 out of 11). While 36,4% responders (4 out of 11) do not use ITIL in their organisations.

6 responders have evaluated ITIL processes from the information security management point of view. All 6 responders stated that ITIL is not tuned for information security management but it has to be fine-tuned based on each organisations work and sphere of service provision. It was also stressed that ITIL is valuable from the point when it is isolating different functions (security from basic management) and process (incident management from marketing).

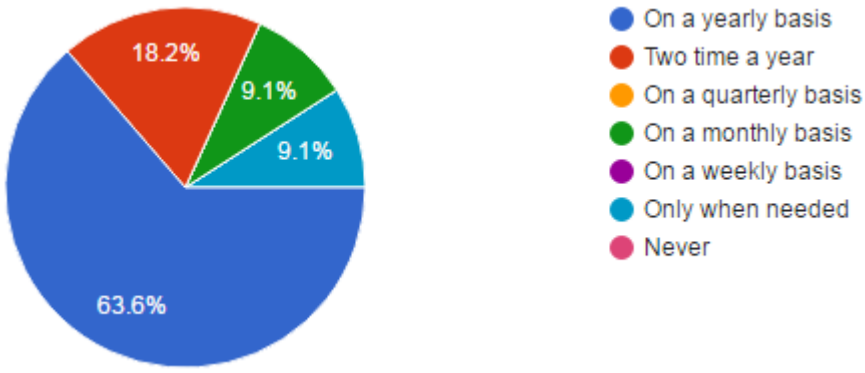
Table 3 Evaluation of technical knowledge needed to execute special functions

Special functions	Points achieved (the more the better)	Average score
Configuration manager	39	3,55
Incident manager	45	4.10
Change manager	37	3,36
Information security officer	47	4,27
IT department manager	44	4
Mid-level managers	29	2,64
CEO	35	3,18

Evaluation of technical knowledge was one of the most important to understand from the point of information security management. While the question was to evaluate from 1 to 5 the level of technical knowledge needed for mentioned functions to be carried out, 1 being no technical skills needed and 5 representing an IT expert. The evaluation showed that 3 functions have to have technical skills higher than average – Incident manager, Information security officer, and IT department manager. Most obviously this can be interpreted as the key functions in information security management sphere. It is worth to notice that other functions should have good technical skills to carry out their functions (from 3,18 to 3,55) – CEO, Change manager and configuration manager. It is worth to notice that mid-level managers had the lowest evaluation of technical knowledge needed from the information security point of view. As in the question before one of the reasons for information leakages was personnel's lack of knowledge and training – answers provided for the question above enforce this position and stress the need of separation of information security management functions and the expertise needed to carry out those functions.

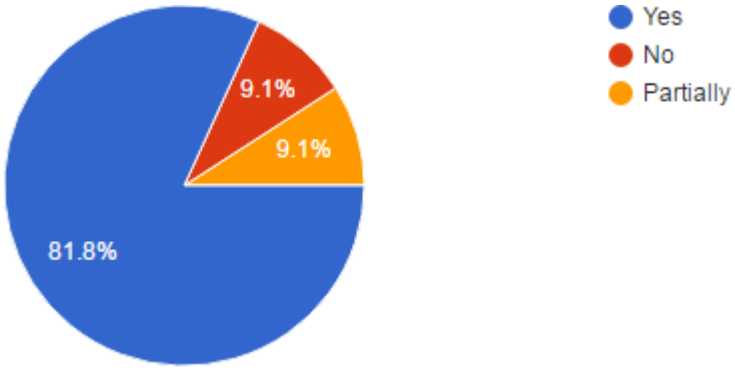
Question No. 10 involved evaluation of risk assessment importance. 90,9% of responders (10 out of 11) have evaluated risk assessment as being very important for their organisations. 9,1% of responders (1 out of 11) mentioned that risk assessment is not important for their organisation.

Figure 22 Frequency of risk assessment execution in a organisation



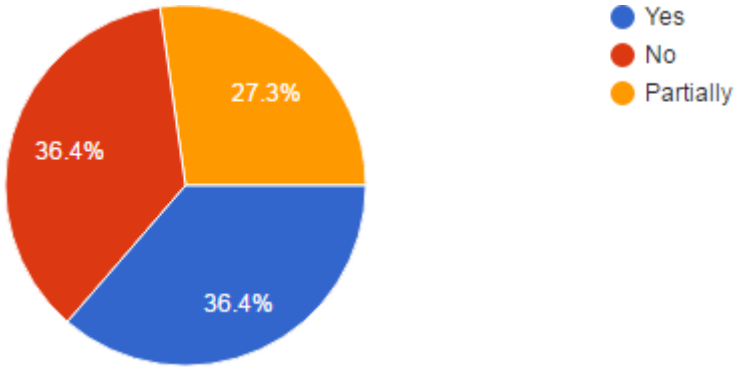
As we can see above risk assessment with different frequency is being carried out in all of the responder's organisations. Majority of responders (63,6% - 7 out of 11) stated that risk assessment in their organisation is being carried out on a yearly basis. 18.2% (2 out of 11) of responder's organisations carry out risk assessment twice a year and only a 9,1% (1 out of 11) carry out risk assessment on a monthly basis and 9,1% (1 out of 11) carry out risk assessment only when needed. From the figures it is possible to evaluate the need of risk assessment but also the need to carry it out in a proper manner (because of its price and human resources consumption). Assessing risks on a yearly basis is convenient, because it may start the change management process to adjust to the changing threats and plan additional budget for the next financial year, but it may lack flexibility in high risk e-businesses like e-banks. While assessing the risk on a weekly basis can be expensive and non-productive as there will be not enough to analyse and act on action points from the risk assessment. It is important to note that each type of e-business has to evaluate the frequency of executing risk assessments based on their information security strategy.

Figure 23 Incident management implementation in responder's organisations



As we can see from the chart above in 90,9% of responders (10 out of 11) organisations Incident management is being implemented when only in 9,1% it is not implemented (1 out of 11). This notes the importance of incident management and on the level of ITIL implementation, because ITIL is the key framework that imposes to have incident management in an organisation.

Figure 24 Security incident management as a part of incident management in responder's organisations



One of negative points that were observed by the author was the lack of security incident management as a port of the organisations incident management process, as this is not stressed in majority of the frameworks and standards. From the answers provided by the responders we can assess that 36,4% of responders (4 out of 11) organisations do not include security incidents in their incident management and 27,3% have it included partially (3 out of 11). Only 36,4% of responders (4 out of 11) have it included in their incident management process. This figures are important because organisations do not tend to be prepared for security incidents while those paying great attention to service provision incidents (outages, service interruptions).

Question 14 addressed the responders to evaluate the flexibility of information security management model in their organisations suitability to different branches of the organisation. 72,8% of responders (8 out of 11) have answered that the information security management models implemented in their organisations lack flexibility and are not suitable for all the branches, when 27,2% of responders (3 out of 11) answered that their information security management models are flexible. Main reasons from the experts were that each branch has to have different processes implemented and there is no one model for large organisations and the responders whom mentioned that their information security management model is flexible mentioned that while assessing the risks on a yearly basis also the information security management model changes based on those threats.

Table 4 Evaluation of importance of difference aspects while creating an information security strategy

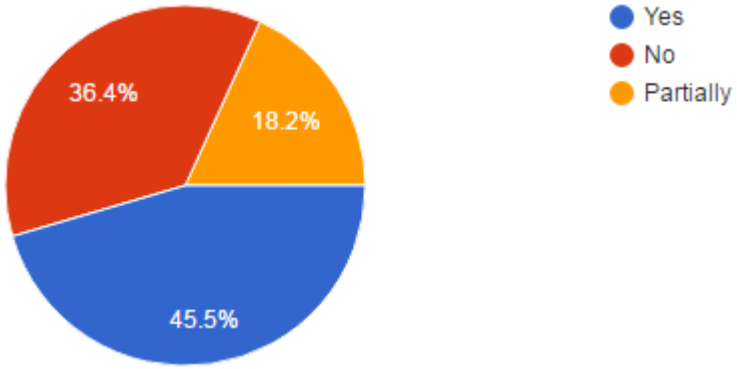
Special functions	Points achieved (the more the better)	Average score
Security constraints	39	3,55
Business needs	53	4,82
User friendliness	42	3,82
Customer conception	48	4,36
Flexibility	38	3,45

Table above presents the evaluation made by the responders to the most important aspects while creating information security strategy for an organisation (each responder evaluated each point from 1 to 5 - while 1 least important and 5 being most important). From the average score above we can see that the most important points are business needs and customer conception of the environment. When security constraints, user friendliness and flexibility are being considered less

important. This can be presented by the ambition of business to create a most proper service or application for the customer that he would not see any security constraints and would have the best experience. This points are important for implementation of security in depth in the organisations starting from the strategy, because finding a compromise between this aspects may lead to a success failure for the organisation.

Question 16 addressed the responders did they encountered a situation when managers without proper technical background were leading technical decisions without understanding their real implications for implementation or maintenance. Based on the answers provided we can see that 36,4% of responders (4 out of 11) answered no and 63,6% of responders (7 out of 11) answered that they have encountered a situation like in the question. This enforces the need of technical knowledge for the management personnel and in particular a change manager which would understand all the implications of the changes arising.

Figure 25 Presents the organisations which have implemented security standards ISO 27000 and 27001



As the chart above presents 45,5% of responders (5 out of 11) organisations have security standards 27000 and 27001 implemented in their organisations with 18,2% (2 out of 11) have them implemented partially and 36,4% of responders (4 out of 11) do not have this standards implemented in their organisations. As we can see from this question and question before concerning the ITIL implementation – companies which personnel was interviewed have implemented either a best practice as ITIL or a security standard ISO 27000 or ISO 27001.

Question 18 asked responders that have ISO 27000 or ISO 27001 implemented to evaluate this standard. Responders 45,5% whom organisations have this standards implemented stated that this is a good baseline for the initial security level build up in the organisation, while the 18,2% of the responders which have it implemented partially tend to evaluate it as mandatory standards from the legal perspective.

5.1. Summary of the results

The interview with IT and information security experts was intended to perform a more in-depth research of the practical knowledge about the information security management frameworks

and standards. Main areas of the interview where the evaluation of: ITIL framework and ISO 27000/27001 standards, technical knowledge of some critical information security positions, risk assessment importance and frequency of its execution, incident management implementations and distinguishing the amount of information breaches. After reviewing all the answers of the responders we can supplement the results gathered while researching the single case study and see the common tendencies in need of implementation of proper information security frameworks and standards, achieving proper technical expertise for information security managers, stressing the importance of risk assessment execution. It is clear that even in enterprise level e-businesses or governmental organisations with proper budgeting information security is one of the critical aspects and one of the key functions to be concentrated on as this in a majority of situations is mission critical.

CONCLUSIONS

In this Master's thesis author has investigated information security management in a more in depth way with concentration on e-business. There were investigated different information security frameworks and standards, security models and tactics how to implement security by design in early phases of organisation strategic planning. Researching the complexity of information security in general and complexity of different types of e-businesses and different organisations all suggestions proposed by the author will be as principals which work for any type of organisation operating in cyber environment.

In order to answer the research problem it was important to evaluate what processes should be implemented in an organisation and how they should be improved for better information security management. Author in the 1'st and 2'nd chapter of the study had examined the importance of risk management, incident management, problem management, change management and continuity management. Researched material stresses a complex view on information security which includes physical, asset, personnel, cyber security implementation in e-business to ensure that the level of ambition of the organisation for information security would be achieved. Implementation of this functions and their improvement based on information security strategy goals is critical to achieve the level of ambition that the company has established. It is also important to mention information security strategy creation and its importance being the milestone which determines further steps in design and operations of the organisations processes. Security by design combined with SDLC methodology makes the implementation of information security strategy more appropriate and with positive long term results.

Chapter 4 and 5 are the main chapters of research which was carried out to validate or reject the proposed hypotheses. The final outcome of the research was to confirm all of the hypotheses based

information gathered from the single case study of the enterprise and information gathered by interviewing information security experts.

The conclusions of this research are described below:

1. Lack of information security management in E-business leads to loss of sensitive information, so e-business oriented organisations should implement information security management from the early stages of companies strategy creation. This strategies should have implemented the guidance of the top level managers that the companies would follow a flexible and proactive information security management model which would implement in itself principals like “security by design” and “security in depth” to provide a comprehensive guidance to all companies employees and to higher the responsibility for keeping information secure.
2. Risk management assessment execution on a constant frequency and its trending to information security threats is the essential tool to possess a flexible and ever ready information security model. Assessing the ongoing threats and including them in e-business standard procedures and guidelines for the employees will help the organisation to lower the probability if not of an event occurring but lowering the possible damage which that event may impose. Risk assessment management should not only include the full spectre of the possible risks but also the critical assets that organisation has to protect (infrastructure assets, information assets, services).
3. E-businesses should implement critical service management functions in their organisational structure to ensure that incident management, problem management, change management and continuity (continual service improvement) management would be conducted (as recognised by ITIL best practices). Functions presented are not exhaustive, but from the information analysed in this research they pointed out as the most critical to enforce information security in an organisation. It is important to stress that implementation of this service management functions should be done in such a way that they are tailored to the organisations operational environment (analysing by SDLC methodology) and would include management of security issues like security incident management, cyber incident management, information leakage incident or problem management (as stated by ISO 27000 and 27001 standards).
4. While technical or organisational aspects of information security management are important it is still critical to prepare employees for carrying out their information security duties. It is important to establish expertise and to connect both managerial skills and technical expertise of managers which operate in cyber environment. Lack of technical skills creates a risk that the management may under estimate the implications that may appear in the decision making process and without desire undertake an extra risk.
5. Information security management should be seen as an overarching process which fits in it all critical aspects like cyber security, physical security, employee security, data network

security. This is important to understand what e-business should achieve and to concentrate on information security in general. This viewpoint will help managers to understand that achieving information security is a collective task.

This research provides many implications not only to practical but also to the theoretical part of information security management and this should be addressed by adopting the results based to the organisations to which this results may be applied.

Further research on this topic is needed to be prepared for the ever changing environment of e-business and the cyber environment in which e-business operates.

Student:
Mr. Tomas Mogodia,

REFERENCES

1. 2016 Cost of Data Breach Study: Global Analysis (2016). IBM and Ponemon institute LLC.
2. 2016 Cost of Data Breach Study: Impact of Business Continuity Management (2016). IBM and Ponemon institute LLC.
3. Adams J. (2007). Research Methods for Graduate Business and Social Science. SAGE Publications.
4. Agarwal R. (2000). Individual Acceptance of Information Technologies. Educational Technology Research and Development.
5. Alasuutari P. (2004). The globalization of qualitative research, published in Qualitative research practice by SAGE publishing.
6. Albuquerque O., R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati, F., & Tai-Hoon, K. (2014). A Layered Trust Information Security Architecture, Sensors.
7. Alleyne N. (2016). Building a forensically capable network infrastructure. Accessed 2016-10-04. From https://www.sans.org/reading-room/whitepapers/modeling/building-forensically-capable-network-infrastructure-37212.
8. AMBINDER M. (2013). NSA's Org Chart. Accessed 2016-10-01. From http://www.defenseone.com/ideas/2013/08/what-nsas-massive-org-chart-probably-looks/68642.
9. An Analysis of information theft statistics in the USA (2016). Accessed 2016-06-25. From http://www.iii.org/fact-statistic/identity-theft-and-cybercrime.
10. Bickmanm L., Rog J. D. (1998). Applied social research methods. SAGE publishing.
11. Boeije H. (2010). Analysis in qualitative research. SAGE publications.
12. Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. Information Security Journal: A Global Perspective.
13. Cable Installation at NSA Facilities. Document Number: X312-061-1006. Rel. date 2008-09-25.
14. Calder A. (2005). A business guide to Information security. London and Sterling.
15. Carvajal Vión J. F. (2016) Cyberspace. Accessed 2016-10-12. From http://www.indracompany.com/en/blogneo/cyberspace-challenge-ciso.
16. Ceroni J., Moghaddam M., Nof Y. S., Jeong W. (2015). Revolutionizing Collaboration Through E-work, E-business, And E-service. Springer publishing.
17. Chaffey D. (2007). E-business and E-commerce Management: Strategy, Implementation and Practice. Pearson Education.
18. Construction and Management of Sensitive Compartmented Information Facilities, Version 1.2, Document Number ICD/ICS 705. Rel. date 2012-04-23.

19. Cooper R. D., Schindler S. P. (2014). Business research methods. McGraw-Hill Irwin publishers.
20. Corbin J., Strauss A. (2008). Basics of qualitative research. SAGE publications.
21. Davies M., Hughes N. (2014). Doing a successful research project: using qualitative or quantitative methods. Palgrave Macmillan.
22. Durbin S. (2016). Insiders are today's biggest security threat. Accessed 2016-10-12. From http://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin.
23. Esposito R., Cole M. (2013). How Snowden did it. Accessed 2016-10-12. From http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160.
24. Field generation and over-the-air distribution of COMSEC key in support of tactical operations and exercises. Document number: NAG-16F. Rel. date 2001.
25. Frisken, J. (2015). Leveraging COBIT to Implement Information Security (Part 3). COBIT Focus.
26. Gerring J. (2007). Case study research: principles and practices. Cambridge University press.
27. Gerring J. (2012). Social study methodology: a unified framework. Cambridge University press.
28. Gordon A., Certified Information Systems Security Professional's CBK, ISC, 2015,
29. Greenwald G. (2014). No Place to Hide Edward Snowden, the NSA and the Surveillance State. Penguin Group.
30. ISACA (2016). Accessed 2016-09-04. From http://www.isaca.org/about-isaca/Pages/default.aspx.
31. ISO/IEC 20000-1:2011.
32. ISO/IEC 27000:2009(E).
33. ISO/IEC 27001:2013(E).
34. ISO/IEC 27003:2010(E).
35. ITIL® Continual service improvement (2011). Best management practices publishing.
36. ITIL® Service design (2011). Best management practices publishing.
37. ITIL® Service Operation (2011). Best management practices publishing.
38. ITIL® Service strategy (2011). Best management practices publishing.
39. ITIL® Service transition (2011). Best management practices publishing.
40. Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. MIS Quarterly Executive.
41. La Monica P. R. Sony hack sends stock down 10% in past week (2014). Accessed 2016-10-12. From http://money.cnn.com/2014/12/15/investing/sony-stock-hack.

42. Laudon K. C. and Laudon J. P. (2005). Essentials of business information systems. Pearson Prentice hall.
43. Lewis, L. (2016). Cyber Center: Practical Strategies for Developing a Cyber-Incident Plan. Business Law Today.
44. Lomas E. (2010). Information Security Risk Management: Handbook for ISO/IEC 27001. Records Management Journal, Vol. 21 Iss: 3.
45. Matthew M. A. (2009). The Secret Sentry. Bloomsbury Press.
46. Miller R., Maxim M. (2015). Dealing with insider threats to cyber-security. CA Technologies, Security Management.
47. Mission & Strategy. Accessed 2016-10-11. From https://www.nsa.gov/about/mission-strategy.
48. Mulazzani F., Sarcia S. A. (2011). Cyber Security on Military Deployed Networks, 3rd International Conference on Cyber Conflict. CCD COE Publications.
49. National information systems security (INFOSEC) glossary NSTISSI No. 4009 September 2000, US DoD
50. NSA structure (2015). Accessed 2016-09-14. From https://admin.govexec.com/media/gbc/docs/pdfs_edit/the_national_security_agency_—_operates_more_than_5.png.
51. NSA's employees security manual. Accessed 2016-10-11. From http://theory.stanford.edu/~donald/NSA.doc.html.
52. Office of Security Services (2006). Accessed 2016-10-12. From http://www.historycommons.org/entity.jsp?entity=office_of_security_services_1.
53. Organizational Structure of the National Security Agency (2013). Accessed 2016-10-22. From http://www.matthewaid.com/post/58339598875/organizational-structure-of-the-national-security.
54. Polygraph Questioning Techniques (2003). Accessed 2016-10-24. From https://www.nap.edu/read/10420/chapter/12.
55. Proprietary research methodology. Accessed 2016-10-01. From http://www.gartner.com/technology/research/methodologies.
56. Sahadi J. (2013). What the NSA costs taxpayers. Accessed 2016-10-17. From http://money.cnn.com/2013/06/07/news/economy/nsa-surveillance-cost.
57. Security by Design Principles (2016). Accessed 2016-10-21. From https://www.owasp.org/index.php/Security_by_Design_Principles.
58. Singh A. N., M.P. Ojha G. A. (2014). Identifying factors of organizational information security management. Journal of Enterprise Information Management, Vol. 27 Iss 5.
59. Swanborn P. (2010). Case study research. SAGE publications.

60. Vacca J. R. (2009). Computer and information security handbook. Morgan Kaufmann publishers.
61. Von Solms, R., Niekerk, J. (2013). From information security to cybersecurity. Accessed 2016-10-14. From http://dx.doi.org/10.1016/j.cose.2013.04.004.
62. What is WikiLeaks (2015). Accessed 2016-10-12. From https://wikileaks.org/What-is-Wikileaks.html.
63. Whitman M. E. and Mattord H. J. (2009). Principles of information security. Thompson course technologies.
64. WikiLeaks Fast Facts (2016). Accessed 2016-10-12. From http://edition.cnn.com/2013/06/03/world/wikileaks-fast-facts.
65. Yin R. (2009). Case study research: design and methods. SAGE publications.
66. Yin R. (2011). Qualitative research from start to finish. The Guilford press.
67. Yin, R. (2016). Case study research: design and methods. SAGE publication.
68. Zeinecke P. (2016). 65 % of internet users in the EU shopped online in 2015. Accessed 2016-10-25. From http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#65.C2.A0.25_of_internet_users_in_the_EU_shopped_online_in_2015.

SUMMARY IN ENGLISH

The topic of this master thesis is both theoretical and practical importance. Due to the examination of both theoretical and practical points of view on information security, the author generated new ground and knowledge and analysed existing information security standards which are addressing information security management. Researched topics analysed information security in a complex way (including all basic dimensions of information security like physical security, cyber security, security incident management, etc.) with concentration for organisations which operate in electronic environment (e-business).

Research was conducted through analysis of a single case study and an interview of information security and IT experts. Research included an analysis of the best practices and international standards while the case study was done based on information leakage incident which happened to a major government organisation which operates in cyber environment.

The object of the research was information security management assurance in E-business. The aim of this research was to confirm either deny the hypothesis which author addressed, that is information security management deficiency in E-business leads to loss of sensitive information and lack of information security management techniques leads to a lack of effective incident management processes in e-business. Objectives of the research included analysis of scientific literature, archived information, official documentation and questionnaire based interview. In the period of the research author analysed numerous international standards and best practices which are industry proven standards.

Final outcome of the research confirmed all the proposed hypotheses. While conclusions, addressed that e-business would follow a flexible and proactive information security management model which would implement in itself principals like “security by design” and “security in depth” and stressed the importance of risk management assessment execution on a constant frequency and its trending to information security threats. Key points that were addressed further are the need of service management processes which would be adjusted for security incidents, the importance of balancing technical expertise and managerial skills for personnel which is responsible for information security management/implementation in the organization.

Keywords

Information security management, information assurance, e-business, ITIL, ISO 27000, ISO 27001, incident management, WikiLeaks, NSA, case study.

SUMMARY IN LITHUANIAN

Šis darbas svarbus teorine bei praktine prasme dėl analizuojamos temos naujumo ir svarbos šiuolaikiniame pasaulyje, tai yra informacijos apsaugos valdymas organizacijoje veikiančioje elektroninėje erdvėje. Autorius išanalizavo informacijos apsaugos valdymo geriausias praktikas bei tarptautinius informacijos apsaugos standartus pripažįstamus IT pramonėje. Išanalizavus minėtus šaltinius autorius siūlo kompleksinį požiūrį į informacijos apsaugą, tai yra apimanti fizinį saugumą, kibernetinį saugumą, procedūrinį saugumą, saugumo incidentų valdymą susitelkiant ties e-verslo organizacijomis.

Tyrimo tikslas buvo išanalizuoti informacijos apsaugos valdymo užtikrinimą e-versle. Šio tyrimo pagrindinis tikslas buvo patvirtinti arba paneigti hipotezes, kurias autorius pateikė, tai yra informacijos saugumo valdymo procedūrų trūkumas e-versle sąlygoja konfidencialios informacijos praradimą, bei informacijos saugumo valdymo metodų trūkumas sąlygoja incidentų valdymo procesų trūkumus e-versle. Mokslinio tyrimo eigoje autorius panaudojo teorinius ir empirinius duomenų analizės ir rinkimo metodus bei atliko atvejo analizę. Teorinėje dalyje buvo panaudoti mokslinės literatūros, archyvuose, oficialiuose dokumentuose esančios informacijos analizė ir informacinių technologijų bei informacijos apsaugos specialistų apklausa.

Galutinis autoriaus atlikto tyrimo tikslas buvo patvirtinti suformuluotas hipotezes. Darbo išvadose teigiama, kad e-verslas privalo implementuoti savo veikloje iniciatyvų bei lankstų informacijos apsaugos modelį kurio sudėtinės dalys būtų principai kaip "saugumas projektuojant" (ang. – security by design) ir "saugumas nuodugniai" (ang. – security in depth). Taipogi svarbus aspektas yra rizikos valdymo vertinimo vykdymas ir šio vertinimo pastovus pasikartojantys vykdymas bei pateikiamų rizikų įvertinimas bei diegimas į informacijos apsaugos valdymo sistemas siekiant sumažinti galimo pažeidžiamumo riziką. Kitos svarbios išvados yra paslaugų valdymo procedūrų kaip incidentų valdymas, pakeitimų valdymas, poreikio valdymas implementavimas kasdieninėje e-verslo veikloje bei techninių ir valdymo kompetencijų subalansavimas tarp personalo atsakingo už informacijos apsaugos organizavimą.

Raktiniai žodžiai

Informacijos apsaugos valdymas, informacijos saugumo užtikrinimas, e-verslas, ITIL, ISO 27000, ISO 27001, incidentų valdymas, WikiLeaks, NSA, atvejo analizė.

SUPPLEMENT

A. Interview questionnaire in English

Survey for information security managers/technicians

Information security management interview

This survey is intended for information security experts (IT department heads, Information security specialists, cyber defence technicians) to evaluate industry proven standards and frameworks. The goal of this survey is to evaluate different approaches and frameworks of information security management in a company.

What is your position within the organization? *

1. CEO
2. IT section head
3. Information security section head
4. Cyber defence specialist
5. IT administrator
6. Information security offices (INFOSEC)
7. Other

How many employees are in Your organization?

Short-answer text

Is Your organization falling under "E-business" category?

◯ Yes

◯ No

◯ Partially

Do you have a degree on Information Systems or Telecommunications? *

Yes

No

Has Your organization encountered any information leakages in past 5 years? *

- ◯ No
- ◯ I don't know of any

What do you think would be the main reason for most of the information security breaches (in general)?

Long-answer text

Is Your company following ITIL framework for information security management? *

- Yes
- No
- Partially

Based on Your experience how would you evaluate ITIL processes from Information security management point of view?

Long-answer text

Please evaluate the level of technical knowledge needed for below functions to be carried out? (from 1 to 5 - while 1 being no technical skills needed and 5 representing an IT expert)

Row 1. Configuration manager

Row 2. Incident manager

Row 3. Change manager

Row 4. Information security officer

Row 5. IT department manager

Row 6. Mid level managers

Row 7. CEO

Please evaluate the importance of risk assessment in information security management? *

Long-answer text

How often risk assessment is being conducted in Your organization? *

- ◯ On a yearly basis
- ◯ Two time a year
- ◯ On a quarterly basis
- ◯ On a monthly basis
- ◯ On a weekly basis
- ◯ Only when needed
- ◯ Never

Is incident management implemented in Your organization? *

- ◯ Yes
- ◯ No
- ◯ Partially

Does your incident management include processes to handle security incidents (information leakage, data tampering, network breach, insider threat, other security related incidents)?

Yes

No

Partially

Would You evaluate information security management model implemented in your organization as flexible and right for all of the different branches of the organization? (please provide as detailed answer possible)

Long-answer text

While creating information security strategy for an organization what should be considered more important? (from 1 to 5 - while 1 least important and 5 being most important)

Row 1. Security constraints

Row 2. Business needs

Row 3. User friendliness

Row 4. Customer conception

Row 5. Flexibility

Have You encountered a situation when managers without proper technical background were leading technical decisions without understanding their real implications for implementation or maintenance? (if yes, please describe the situation)

Long-answer text

Are ISO 27000 and 27001 standards implemented in Your organization? *

Yes

No

What is your opinion on this standards from information security management point of view?

Long-answer text