DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF BUSINESS ADMINISTRATION
BUSINESS INFORMATION SYSTEMS PROGRAM
MASTER'S THESIS

ENTERPRISE ARCHITECTURE DRIVEN CYBERSECURITY

Aybars BARS

Supervisor
Assist. Prof. Dr. Ferkan KAPLANSEREN

İZMİR - 2019

APPROVAL PAGE

DECLARATION

I hereby declare that this master's thesis titled as "Enterprise Architecture Driven Cybersecurity" has been written by myself in accordance with the academic rules and ethical conduct. I also declare that all materials benefited in this thesis consist of the mentioned resources in the reference list. I verify all these with my honour.

.. / .. / ….

Aybars BARS

ABSTRACT

Master's Thesis

Enterprise Architecture Driven Cybersecurity

Aybars BARS

Dokuz Eylül University

Graduate School of Social Sciences

Department of Business Administration

Business Information Systems Program

In the contemporary business environment, organizations want to benefit from digital transformation to gain competitive advantage and to create better business value. While the digitalization promises a range of important opportunities, it also brings new cyber threats. Business resilience refers to the ability of being affected negatively as less as possible and recovering the business processes in the most efficient way in case of a cyber incident. Cybersecurity management consists of intertangled and sophisticated activities before, during and after a cyber incident. These activities must align with the business strategy, mission and objectives. Enterprise architecture methodologies align business and information technology strategies by enabling a holistic view of the organization. Failure of enterprise architecture may create numerous cybersecurity issues.

The aim of this study is to reveal the relationship between enterprise architecture and cybersecurity management. To investigate this relationship, a qualitative study is conducted with business executives, technical experts and the employees working in the information technology domain, mostly in large enterprises. This study demonstrates that enterprise architecture driven cybersecurity approach addresses security at the design stage. It is concluded that this approach has significant potential benefits in increasing situational awareness in cybersecurity through a more accurate business impact analysis and enterprise asset management.

Keywords: Cybersecurity, Enterprise Architecture, Business Resilience

ÖZET

Yüksek Lisans Tezi

Kurumsal Mimari Odaklı Siber Güvenlik

Aybars BARS

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

İngilizce İşletme Anabilim Dalı

İngilizce İşletme Bilişim Sistemleri Programı

Günümüzde işletmeler, rekabet avantajı elde etmek ve daha verimli bir iş değeri oluşturmak için dijital dönüşümden yararlanmak istemektedirler. Ancak dijitalleşme bir dizi önemli fırsat vadederken, aynı zamanda yeni siber tehditleri de beraberinde getirmektedir. İş mukavemeti, işletmelerin herhangi bir siber olaydan olabildiğince az etkilenerek, iş süreçlerini en verimli şekilde iyileştirebilme yeteneklerini ifade eder. Siber güvenlik yönetimi, olası bir siber olay öncesindeki, esnasındaki ve sonrasındaki, birbirleri ile iç içe geçmiş, karmaşık faaliyetlerden oluşmaktadır. Bu faaliyetler, işletmelerin iş stratejisi, misyonu ve hedefleriyle uyumlu olmalıdırlar. Kurumsal mimari metodolojileri, organizasyonu bütünsel bir bakış açısıyla görmeye olanak sağlayarak, iş ve bilgi teknolojileri stratejilerini uyumlandırırlar. Kurumsal mimari kaynaklı sorunlar çok sayıda siber güvenlik sorunu yaratabilirler.

Bu çalışmanın amacı, kurumsal mimari ile siber güvenlik yönetimi arasındaki ilişkiyi ortaya koymaktır. Bu ilişkiyi araştırmak için, çoğunluğu büyük işletmelerde çalışan üst düzet yöneticiler, teknik uzmanlar ve bilgi sistemleri etki alanında çalışan personel ile nitel bir çalışma gerçekleştirilmiştir. Bu çalışma ortaya koymuştur ki kurumsal mimari odaklı siber güvenlik yaklaşımı, güvenliği tasarım aşamasında ele alır. Bu yaklaşımın, daha doğru bir iş etki analizi ve kurumsal varlık yönetimi ile siber güvenlikte durumsal farkındalığı artırmada potansiyel faydalarının bulunduğu sonucuna varılmıştır.

Anahtar Kelimeler: Siber Güvenlik, Kurumsal Mimari, İş Mukavemeti

ENTERPRISE ARCHITECTURE DRIVEN CYBERSECURITY

CONTENTS

CHAPTER TWO
CYBERSECURITY FOR BUSINESS RESILIENCE

CHAPTER THREE
ENTERPRISE ARCHITECTURE FOR INTEGRATED SECURITY

CHAPTER FOUR

ENTERPRISE ARCHITECTURE AND CYBERSECURITY RELATIONSHIP EVALUATION

ABBREVIATIONS

APT	Advanced Persistent Threat
BIA	Business Impact Analysis
BMI	Business Model Innovation
CIS	Center of Internet Security
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
CSF	Cybersecurity Framework
C4ISRAF	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Architecture Framework
DDOs	Distributed Denial of Service
DoDAF	Department of Defence Architecture Framework
DOS	Denial of Service
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GRC	Governance, Risk Management and Compliance
HITRUST	Health Information Trust Alliance
IA	Information Assurance
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet of Things
IIoT	Industrial Internet of Things
IPS	Intrusion Protection System
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Science and Technology
PCI DSS	The Payment Card Industry Data Security Standard

SABSA	Sherwood Applied Business Security Architecture
SCADA	Supervisory Control and Data Acquisition
TOGAF	The Open Group Architecture Framework
SP	Special Publication

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

INTRODUCTION

Rapidly evolving digital technologies, in other single word, digitalization shapes every domain of our lives: the way we think, what we do, how we do, the way we live and even the way we war in location independent battlefields with no borders. Digital technologies change the way we work thus, not surprisingly it forms the businesses at all levels. This is not a mystery that business and information technology (IT) transform each other mutually. The new digital era creates its own cyber ecosystem with techno-ecology and digitized environment. Today, everything is going mobile and cloud. Digital communication restructures our lives constantly.

Information technology is one of the most powerful value driver for organizations. Business value such as novelty, competitive advantage, product and service quality, brand value, customer and stakeholder trust, etc. is one of the most important concern for organizations and is more than absolute economic value. Enterprise architecture methodologies and frameworks are applied for aligning IT strategy with business strategy for better business value. A digital enterprise can integrate information, process, technology and people as an asset so it works more efficiently in a harmony and thus it can make advantages to their competitors. When it is put into practice properly, by choosing the right technology to deliver digital transformation, it is obvious that enterprises can create new business values inside and outside of the organization. Digital transformation is not an option and so it shall be almost an imperative virtually for every organization.

Nearly all information systems confront cybersecurity incidents. The cyberattacks are increasing in number and the sophistication of them are growing every single day. In 2012, February, Former Federal Bureau of Investigation (FBI) Director Robert Mueller included in his statement “I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.” (Nielsen, 2012). Cybersecurity threats such as data breaches are often severe to the organizations. This issue is prioritized worldwide in both public and private sectors, nationwide and internationally. Every country makes significant efforts to ensure cyber hygiene, especially in Supervisory Control and Data Acquisition

(SCADA) networks. International actors such as institutions, organizations and groups consistently conduct studies to define cyber controls, white papers, best practices, frameworks and they build standards. Cybersecurity is a big business with lots of hats from white to black, meaning from serviceable professions to the malicious ones that everyone should worry about their activities. In IT industry, cybersecurity companies and the security solutions in both hardware and software are on the rise due to the need. But even lots of active endeavour is being done in this subject, it is not well enough to securitize the assets.

Cyber resilience is the ability of durability, adaptability and recovery by accepting the existence of cyber risks but focusing on cyber incident management due to business resilience. Business continuity planning is the core activity of business resilience which is vital for every digital enterprise. When the security concern is an afterthought, the consequences of a cyberattack to an enterprise could possibly endanger the business continuity and business value. Understanding the nature of the problem is important. Focusing on only yesterday's problems is not a solution.

Cybersecurity endeavours consist of intertangled and challenging activities that concern both business, IT and security roles in the organization therefore every enterprise needs to have a relevant, state of the art cybersecurity strategy subsumes involved stakeholders solidly. These activities are asset management, identification of possible threats and vulnerability analyses, devise incident response plans, continuous monitoring and log management for diagnosing anomalies and determining adversary activities. Raising awareness about cybersecurity and how cyberattackers approach, cyber resilience status evaluation, risk mitigation, recovery plans include processes and procedures to ensure timely restoration of assets affected by cybersecurity events are also included mentioned activities above.

This study has shown that, enterprise architecture methodologies can be beneficial in terms of conducting perpetual business impact analysis and assuring business continuity due to an interruption caused by a cyber incident. The respondents to the interviews and surveys expressed the opinions about importance of asset management and reducing complexity. According to the interviews, enterprise architecture, as a self-knowledge tool, clarifies layered security, creates common language and common point of view, leds to better planning and better business

strategy alignment. Interviewees expressed that seeing big picture in the organization and avoiding unnecessary resource utilization is important in terms of consumerization of IT and cybersecurity solutions. Common consideration is that enterprise architecture methodologies provide better business and security strategy alignment.

The first part of this thesis focuses on the importance of cybersecurity for businesses in terms of main business concerns, challenges, the problem area of managing risks and the common and most impactful threats that businesses face. In the second chapter, cybersecurity itself and its aspects are defined with the concepts of information security and Information and Communications Technology (ICT) security. Main cybersecurity management activities that organizations conduct are studied in detail in this chapter. In Third chapter, enterprise architecture methodology and framework concepts are discussed. Common enterprise architecture methodologies and frameworks are examined due to cybersecurity management integration, which is the main purpose of the study. In Fourth and the last chapter, the use of common enterprise architecture methodologies is reviewed. Awareness and perceptions of how beneficial is enterprise architecture for enterprise cybersecurity is discussed and analysed with a qualitative study. Moreover, expectations, thoughts and recommendations are collected from elite executives and specialists from digitally mature, top level organizations.

CHAPTER ONE

CYBERSECURITY FOR BUSINESSES

1.1. BUSINESS CONCERNS

Information technology is both enabler and enhancer virtually for almost all business functions. The expansion of this technological dependence alters the business concerns in terms of cybersecurity which is integral part of business continuity and business value creation. Additionally, IT governance, risk management and compliance (GRC) makes cybersecurity the subject of management (Singh, Picot, Kranz, Gupta, & Ojha, 2013: 225). In this chapter, these concerns are discussed due to main cybersecurity and administrative issues that pressures at both technical experts and business executives.

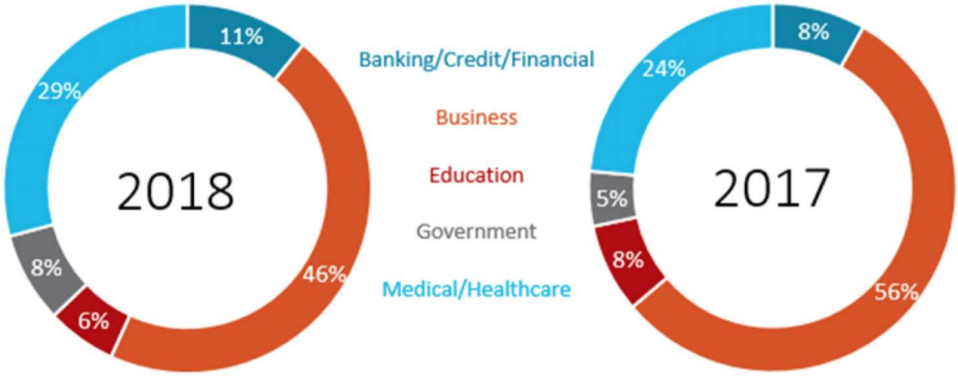
Data driven approaches give significant opportunities to the businesses. In order to realize the business, the information and the data flows in the enterprise must be secured during process, transmit and at rest. Data is the new source of economic and social value. Businesses use data analytics from better customer experience to enhanced productivity. Big data is a catalyst for digital revolution (Burmeister et al., 2019: 6052). In fact, we are part of the big data with our digital fingerprints in this interconnected world with our choices, likes and dislikes. Even more, it is almost impossible being isolated from this new domain for human being that use any Internet of Things (IoT). Personal data is in the cloud and transfers every millisecond; mobile applications, online shopping, reservations, even votes. Not the only data is big but also the risk of being compromised is getting bigger. However, big data is a value creator for businesses, there is a dark side of being exploited (Burmeister et al., 2019: 6052).

Cybersecurity related subjects are confidential virtually for all organizations. So it is generally inconvenient to collect incident statistics from the first hand for even research purposes. This is only itself shows that the importance of cybersecurity is significant for businesses and for all organizations in public and private sectors.

Following base of information collected from different researches, surveys and reports from trustful resources are not in a chronological order, nor in a subject order but the main intention is condition assessment.

As shown at Figure 1 provided by Identity Theft Resource Centre, even some decrease is seen at the total share, data breaches still threaten business the most compared to other sectors. According to recent regulations like General Data Protection Regulation (GDPR), and huge legal enforcement as consequence, data and information security is a business concern like never has been before. Identity thefts, data breaches and the other cyber incidents that threaten businesses will be analysed in depth at section 1.3. The definition of cyber incident, information security and other related taxonomies that clarify the cybersecurity concepts are scrutinized in Chapter 2.

Figure 1: Reported Data Breach Shares by Industry, US



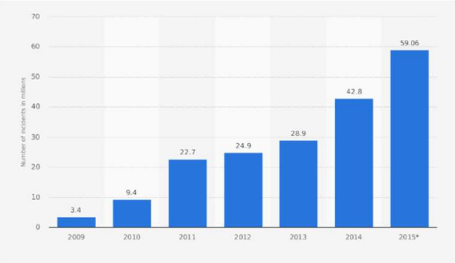
Source: Identity Theft Resource Center, *End of Year Data Breach Report*, 2018:13

Cyber incident is an "hush-hush" subject for any organization and it is a matter of prestigious, for both external stakeholders and consumers that looks for trusted third parties. The survey findings presented of this dissertation in Chapter 4 shows that, loss of prestige is one of the main concerns of business. The other concerns are shown in the same chapter in detail. On the other hand, it is not a secret that cybersecurity teams are somewhat isolated in the organization. In some cases, it causes a problem for enterprise communication and this subject will be discussed in Chapter 1.2.4.

In Figure 2, PricewaterhouseCoopers (PwC) International accounting firm professionals published a global cyber incident report at Statista interface, which has

over a million statistics collected from 170 industries and over 1.5 million registered users. It can be concluded that the quantity of cyber incidents is growing in years worldwide.

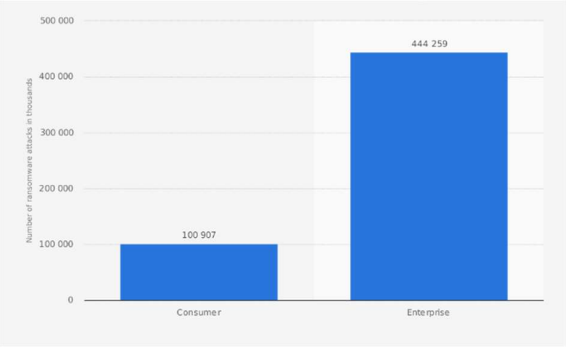
Figure 2: Cybersecurity Incidents Worldwide, Between 2009 and 2015



Source: https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/ (26.10.2018)

In Figure 3, another incident report conducted worldwide by Symantec, which is a software firm that produces information systems security products and information management solutions. The report that published in Statista shows that, enterprises are more than 4 times more at risk compared to individuals, at least for ransomware attacks. This malicious actor, ransomware, is a thrilling concern for businesses and the definitions explained in depth at Chapter 1.3.6.

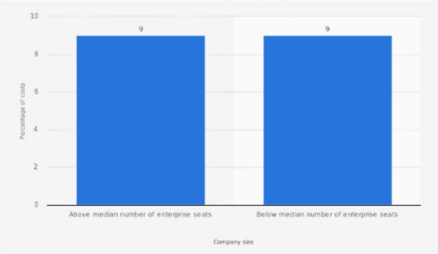
Figure 3: 2018 Report, Ransomware Attacks Worldwide by Market



Source: https://www.statista.com/statistics/983248/number-ransomware-attacks-market-worldwide/ (20.04.2019)

In Figure 4, Ponemon Institute which conducts researches nearly for two decades and Hewlett – Packard (HP) Enterprise Institute examined the companies in the US by size and categorized them in two class in 2015. The companies are sorted with above median, the companies who has more than 13.251 enterprise seats and below median with less seats. The percentage of costs with 9 percent show no difference between company size in terms of malware attacks. On the other hand; the ability of the support organizational security requirements is influenced by the organization size (Abernathy & McMillan, 2018: 28).

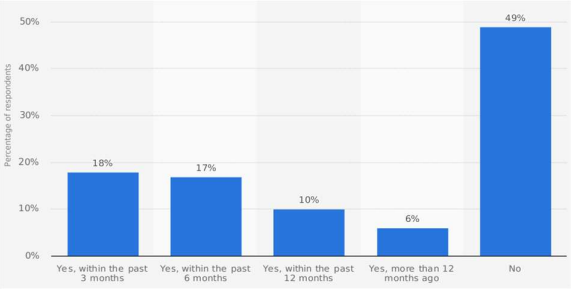
Figure 4: Cyber Crime Damage Caused by Malware and Enterprise Level



Source: https://www.statista.com/statistics/193447/financial-damage-caused-by-malware-for-us-companies/ (14.10.2018)

Figure 5, shows that every 1 of 2 SMEs face with ransomware incident at least one time recently. According to the report conducted between September 2016 and 2017, nearly every 2 of 10 companies experienced ransomware attacks in the past three months. Among small medium enterprises (SMEs) in US.

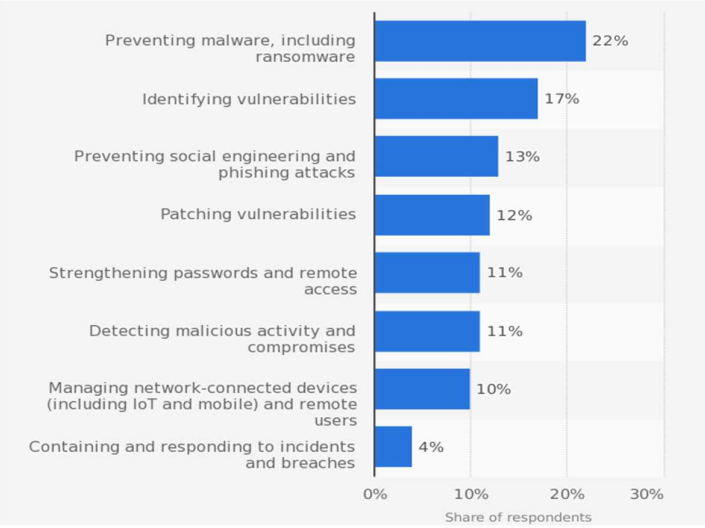
Figure 5: 2017 Small Medium Enterprise Ransomware Report



Source: https://www.statista.com/statistics/701282/ransomware-experience-of-companies/ (20.04.2018)

According to Figure 6, the survey conducted worldwide with IT professionals in the field; preventing malicious codes is the most pressure on IT staff. The technical aspects of cyberattacks like malware is discussed in Chapter 2.2.2. and the cybersecurity protection function is detailed 2.3.2. One step backward, identification of vulnerabilities which is the first and the vital step for cybersecurity management is explained in Chapter 2.3.1. Figure 6 indicates other relatively big struggles for businesses to ensure cybersecurity.

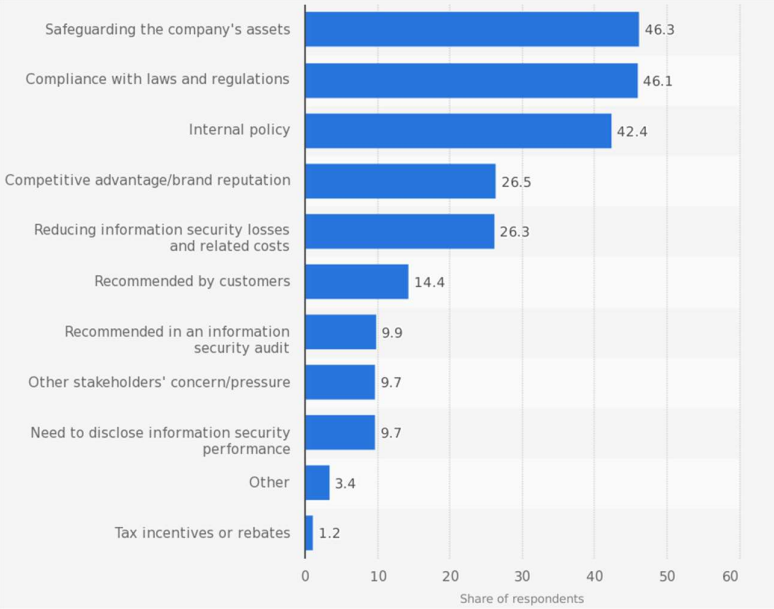
Figure 6: The Pressure of IT Security Tasks, Worldwide



Source: "https://www.statista.com/statistics/709789/most-pressing-global-cyber-security-issues/" (21.06.2019)

In Figure 7, Norwegian consultancy firm DNV GL's survey, conducted through 486 respondents in Europe. According to the research, major reason of taking initiative in information security is safeguarding the company's assets. Solms et al. explained the asset as absolutely anything and anyone in cyberspace (2013:100). Information, one of a business asset itself is still a top priority but it is not limited with information security. In the same figure, it involves whole cybersecurity functions with business asset security, compliance and regulations, policies, costs, customer demands, etc.

Figure 7: Logic of Information Security Initiatives, 2015



Source: https://www.statista.com/statistics/555250/main-reasons-companies-took-information-security-initiatives-in-europe/ (01.10.2018)

1.1.1. Business Continuity

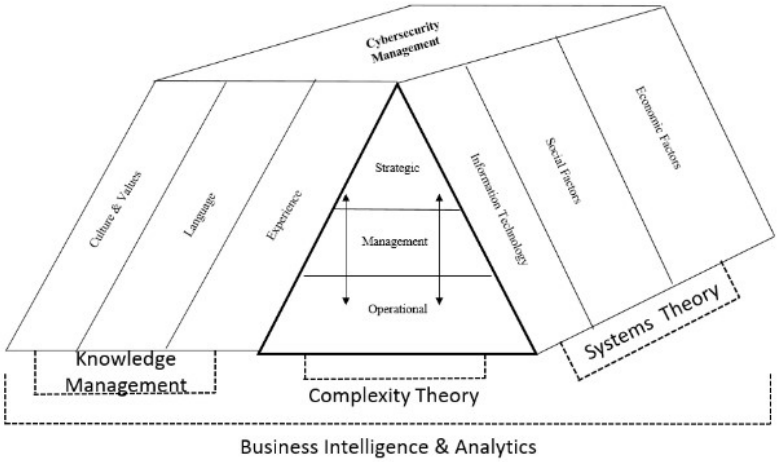
Business continuity is all about business resilience. Information systems and related technologies support missions and virtually all business functions rely heavily on them. It is needed to plan and execute the involving procedures to keep systems operational without interruption due to business resilience (Gantz, 2013) .

Continuity of operations is seen as an economic perspective of the businesses like finance, legal, etc. from Systems Theory (Tisdale, 2015: 195). But business continuity is not limited with the economic perspective, it includes both social perspective like human resources and information technology perspective such as capabilities, performance, enabling and enhancement in the organization.

In Figure 8, Complexity Theory adds different layers to explanation with strategic, management and operational layers (Tisdale, 2015: 196). In the field, it can be seen as strategic, operational and tactical levels or layers. According to the same figure, knowledge management is also an integral part of the cybersecurity

management due to business continuity with experience, language, values and culture. This classification gives an idea about the social aspects of cybersecurity.

Figure 8: Cybersecurity Management Framework



Source: (Tisdale, 2015: 196)

Threat actors can aim to stop business activity that's why cyber resilience strategies include business continuity procedures and risk mitigation plans. In technical manner, denial of service attacks may first come to mind. In Verizon report, denial of service attack defined as any attack that compromises information and communication technologies included applications. These attacks can overwhelm the system and the performance degrades, services may interrupt (*Data Breach Investigations Report*, 2018). The threat landscape is discussed in detail at Chapter 1.3.

1.1.2. Business Value

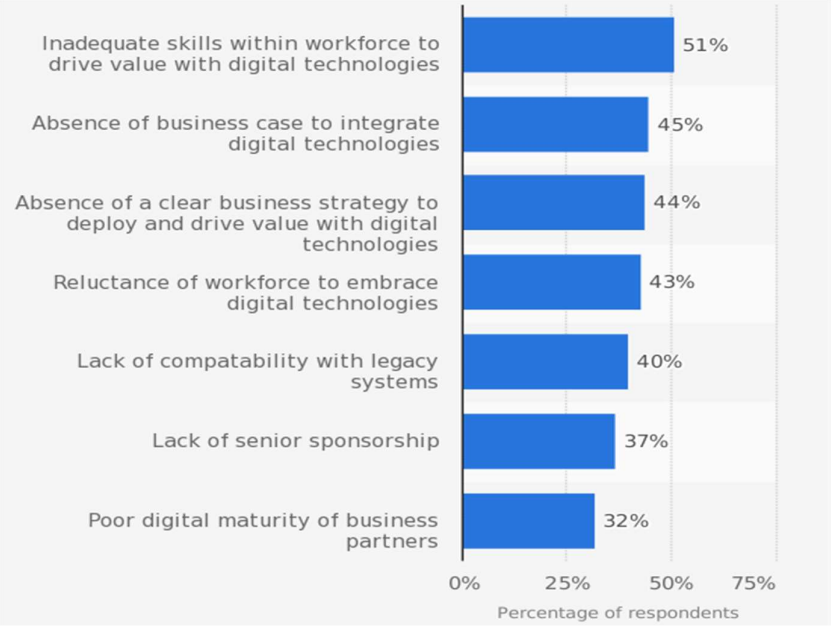
Business value is strongly connected with productivity, innovation, resilience and reliability. According to Schumpeter's theory, value creation is realized by innovation and the technology that plays important role due to creating new production methods and products (Amit & Zott, 2001: 497). Digital opportunities allow global industries to be more reactive, productive and flexible (Rachinger, Rauter, Müller, Vorraber, & Schirgi, 2018: 2). In this concept there are some expressions that can be used interchangeably as follows: digitization, digitalization and digital transformation.

While digitization means that converting analogue data into digital format, digitalization is defined as realizing of the digital opportunities. Digitization is the framework of digitalization. But moreover, digital transformation, is explained as restructuring the economies, organizations and society on a higher level by digitalization. Digital era is seen as a new economy, new society and the new culture (Brennen & Kreiss, 2016: 5). According to the Rachinger et al. (2018:10) business value creation is strongly influenced by digitalization. Digitalization makes the technological innovation cycle shorter. When this cycle becomes shorten, businesses need to adopt and adapt the new technologies to their business model. Business model innovation (BMI) focuses on both addressing new technologies and process innovation (Rachinger et al., 2018: 12).

Business value creation is strongly related with business and information technology alignment. Enterprise architecture (EA), resolves the organization into business, application and technology layers in perpendicular way. EA also represents the organizations' "as is" and "to be" architectures (Engelsmana, Quartelc, Jonkersa, & van Sinderen, 2011: 10). In this manner, enterprise architecture methodologies gain more importance in the concept of digital transformation, business model innovation and business value creation. Cybersecurity is a determinant carrying out the technologies due to digitalization. When done correctly, the contribution of enterprise architecture artefacts such as human beings and technical aspects (Proper et al., 2010: 58) and cybersecurity functions, synergy can be created to bring about better business value.

Figure 9 demonstrates the survey conducted with executives and supply chain managers, worldwide. According to the 900 respondents in the survey, skilled workforce gap is the biggest problem in difficulties with the creating better business value. Other challenges such as business and digitalization alignment in design, adequate strategy that supports digital technologies in order to create better business value, hesitating from new technologies, compatibility issues with older systems, insufficient leader sponsorship and the third parties' inadequate digital maturity are shown in the figure.

Figure 9: Challenges in Creating Business Value, 2018



Source:https://www.statista.com/statistics/979191/challenges-to-value-in-technology-life-sciences-executives/ (07.01.2019)

Companies try to protect themselves from cyber threats by restrictive and protectionist approach but while restricting some features it is experienced that the technology cannot be extracted well enough to contribute business value (Kaplan, Bailey, O'Halloran, Marcus, & Rezek, 2015). There must be an advantageous trade-off between restrictions and promotions of technology usage. At this point, enterprise architecture driven cyber security gains importance again. Adequate and conscious cybersecurity strategy not only protects the organization but also supports to extract maximum from paid technology to create business value.

1.1.3. Governance, Risk Management and Compliance (GRC)

Governance is a very a very inclusive term and the concept is closely related with business value mentioned previous chapter and risk management. Compliance to regulations is another subject of governance in terms of making sure that there is nothing missed in requirements (Rohmeyer & Bayuk, 2018: 124). According to Singh et al. (2013:226) cybersecurity is a management issue, not only a technical

responsibility. Enterprise's getting more engaged between customers, other business partners and outsourced operations largely with information technologies. When technological improvements cause much more diversity in the perimeter, it causes more complexity and information systems related risk are increasing eventually (Rot, 2009: 1). Different IT solutions serves different business processes. Sometimes these processers are successors of each other's so when one assets affect by an incident than other systems may be affected. So, another reason that enterprise architecture methodologies may support cybersecurity management is that the methodology strive against fragmentation of the enterprise. It is concluded that, when organization's IT management activity weakly organized, risk management doesn't work well (Rot, 2009: 6).

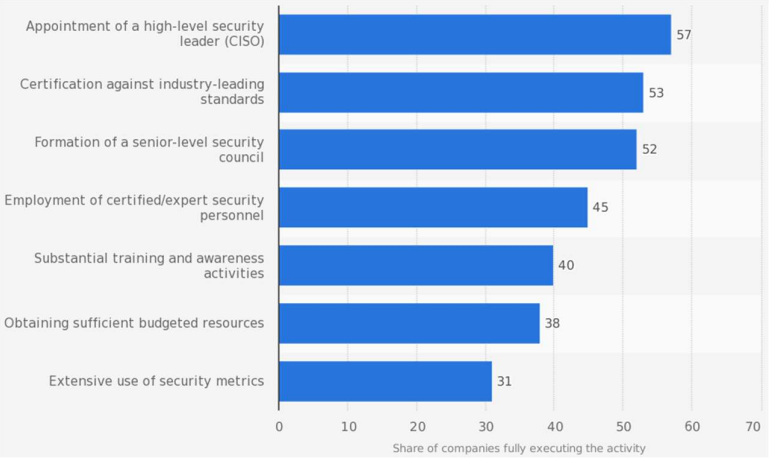
Development and execution of convenient policies has an important role in cybersecurity risk management (Soomro, Hussain, & Ahmed, 2016: 215). Policy management divides into two, managerial and technical ones. Each business should have a comprehensive management architecture. The businesses also need best practices for information security (Chang & Ho, 2006: 345). There are several controls, standards and practices used in the field. Most known ones are National Institute of Science and Technology (NIST) Special Publications (SP), International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) series, The Center of Internet Security, Critical Security Controls, developed by SANS Institute and The Payment Card Industry Data Security Standard (PCI DSS).

Compliances and regulations are also another biggest business concerns due to necessity for alignment in business to business (B2B) data sharing. In the event of incident, adverse consequences such as customer and third party trust, and possible huge fines threatens companies. As an example, almost every company is verdant in terms of General Data Protection Regulation. Burmeister (2019:6053) states that GPDR force the organizations change in enterprise architecture. GDPR is all about data protection and not surprisingly it can be concluded that there is a clear relation between cybersecurity management and enterprise architecture.

Figure 10 shows the most popular cybersecurity governance activities according to the survey among 58 companies in United States in 2015. According to the survey, 57 percent of companies engaged with high level cybersecurity leader and

52 percent of the companies established a senior level security council. While 53 percent of the companies certified for industry leading cybersecurity standards and 31 percent of companies extended use of security metrics, 45 percent the companies joined the survey employed certified, expert security personnel. 40 percent of the companies conducted awareness programs and 38 percent of the companies extended budgets. Figure 10 overall summarizes the importance of top management support, cybersecurity leadership and talent gap

Figure 10: Popular Security Governance Activities by U.S. Companies, 2015



Source: https://www.statista.com/statistics/250361/enterprise-security-governance-activities-deployed-against-cybercrime/ (14.10.2018)

The results mentioned previously in Figure 10 still resonate with the findings in this research in Chapter 4. In the survey, respondents are agreed about the importance of top management support and the leadership in cybersecurity. Likewise, top managers in cybersecurity management expressed the case that, talent gap one of the most challenging issue in cybersecurity activities.

1.2. THE PROBLEM AREA OF MANAGING RISKS

Risk management is integral part of the cybersecurity management and business resilience. Increasing complexity in the enterprise in terms of increasing in

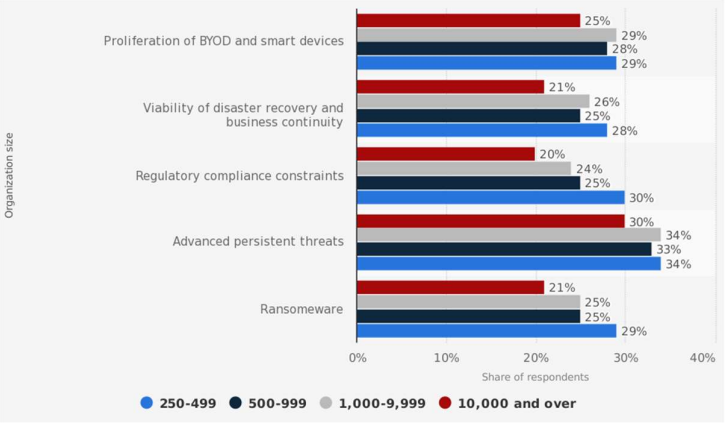
number of systems and technologies and service dependencies make vulnerability analysis difficult. Leadership and management issues like inadequate strategy alignment and poor sponsorship, adverse actions of people in the IT domain, failure in business process design and lack of skilled workforce in the organization who is responsible for cybersecurity activities is the problem area of managing risk (Hoque, Liendo, & Chesson, 2009: 16).

1.2.1. Proliferation of Interconnected Assets

The development in Information Technology and Communications (ICT) allows much more devices to be connected each other and even to the cyberspace. These devices such as sensors, mobile devices, Internet of Things (IoT), and Industrial Internet of Things (IIoT), etc. has a connection feature and they generally can be reached and controlled remotely. Every connected device and the network itself is an asset of the IT perimeter. Some of these devices aren't robust to cyberattacks, some of them needs extra security hardening (*Threatscape Report 2018 Midyear Cybersecurity*, 2018). While having benefit from interconnected world, increasing number and the diversity of connected devices makes it difficult to identify and analyse the vulnerabilities (Choejey, Fung, Wong, Murray, & Sonam, 2015).

Figure 11 shows the survey conducted by Cisco in 2017 with small and medium enterprises (SME). While bring your own device (BYOD) program is encouraged, enterprises sees that as a source of possible cybersecurity risk. Other risks such as Advanced Persistent Threats (APT) and ransomware are studied in Chapter 1.3. One other risk perceived by enterprises in the survey is that disaster recovery plan and business continuity which is mentioned before and regulatory necessities are still concerns for businesses.

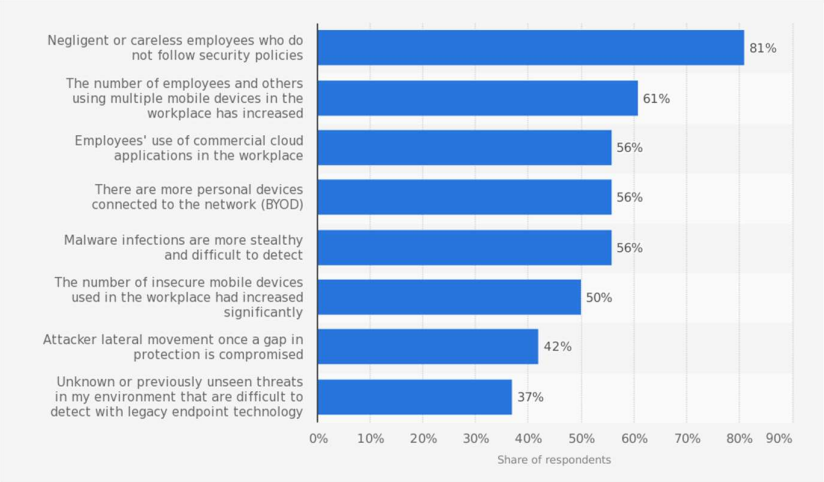
Figure 11: Perceived Cybersecurity Risks, 2017



Source: https://www.statista.com/statistics/803179/perceived-risk-networks-security-threat-organization-size/ (01.04.2019)

The vast majority of connected devices led to endpoint security problems. The survey conducted by Ponemon Institute shown in Figure 12, it is still emphasized the human factor's importance such as negligent and careless behaviours due to endpoint security which is mentioned in following Chapter 1.2.2. On the others hand, commercial cloud applications is another concern for security experts. There is an expression in cybersecurity community: "Cloud is basically someone else's computer." According to the experts, any platform out of the enterprises' own control has malicious potentials. Figure 12 shows that according to the 694 cybersecurity experts, BYOD program one of the biggest threat to enterprise cybersecurity. Mobile devices are hard to keep under control by nature. These devices diversify in hardware and software. But there are several enterprise solutions such as Mobile Device Management for mobile device security that controls these devices remotely by encrypting and even data shredding.

Figure 12: Threats to Endpoints, 2016

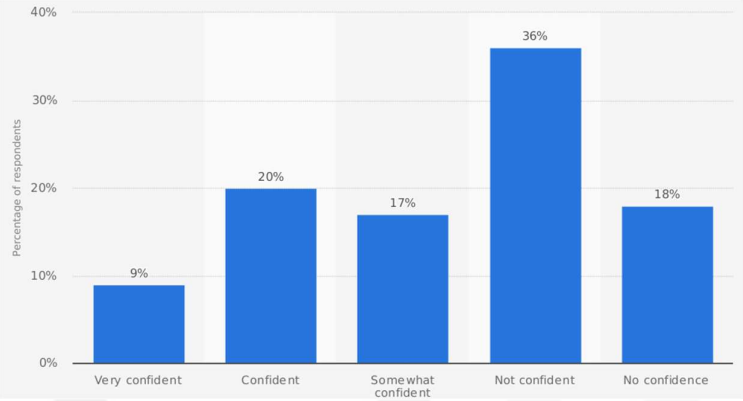


Source: https://www.statista.com/statistics/241268/employee-activities-that-pose-the-greatest-risk-for-cyber-attacks/ (19.04.2019)

1.2.2. Insufficient Awareness and Negligence

Awareness and negligence generally taken as human errors. Recently, human caused incidents are separated from technological cases (Abernathy & McMillan, 2018: 34). Awareness is a managerial activity that impacts the quality of cybersecurity (Soomro et al., 2016: 215). Employees are heavily influenced when top / executive management participate to enterprise cybersecurity program (Hu, Dinev, Hart, & Cooke, 2012). Legal and regulatory measures are needed to address the responsibility of data owners in the enterprise (Warsinke et al., 2019). Enterprise architecture defines the processes with the related business roles, in other words data owners and its enabler and enhancer ICT assets. For adequate awareness training, enterprise architecture is a potential guide with addressing the ICT and the application layers and related roles. Raising in awareness, can results reducing negligent behaviours. But on the other side, some cyber incidents are too sneaky to detect by clients and they can be hunted. Figure 13 represents the survey conducted by Ponemon Institute in United States. More than every one of three of 618 respondents from SME's doesn't feel confident about their employees' awareness in regard to clicking malicious links on the web.

Figure 13: Awareness in Detecting Malicious Links, 2016



Source: https://www.statista.com/statistics/701110/employee-ransomware-detection-us-sme/ (20.04.2019)

1.2.3. Poor Senior Sponsorship

Information technology is increasing online opportunities for businesses but on the other side, the security issues burden the industry. Legal obligations and regulatory requirements, potential losses including business disruption, reputational damage are some motivation factors execution of risk management decisions. Cybersecurity risk treatment execution fails sometimes because of some factors, such as funding, human resources, etc. The aspects of risk management are studied but mostly in a technical manner. Recently, the researches draw attention to leaders' role in cybersecurity risk management (Soomro et al., 2016: 215). Executive management's interest and involvement is vital and the most determinant factor at cybersecurity management program is top management support. (Ezingeard & Bowen-Schrire, 2007: 53; Ma, Schmidt, & Pearson, 2009: 58; Knapp, 2014: 327). Nearly all the cybersecurity experts are agreed that senior leadership has to involve defence in depth approach with policies and procedures (Carey & Jin, 2019: 48). When top management involve policy formulation, the effectiveness of information security increases (Kwon, Ulmer, & Wang, 2013: 219). Sigler (2018:259) also emphasizes the importance of leaderships' role for addressing the culture in terms of enterprise security. Sherwood et al. (2009:2) states the advantages of enterprise architecture methodologies in collaboration between business leadership and technology strategists due to realize the potential of

the enterprise by business focused approach for better business performance and cybersecurity.

Table 1 shows several aspects of management having an important role in cybersecurity management. and second column of the table shows the number of articles that mentioned related concepts.

Table 1: Business and Cybersecurity Related Literature Review

Subject	Number of articles
Management role is critical for Information Security	12
Management role in business IT alignment and security issues	5
Management role in enterprise information architecture	3
Management role in information infrastructure development	4
Effective information security policy, awareness and training impact on information security management	13
Role of human factors in information security management	8
Information security should be a board level issue	4
Employee role in information security breaches	3
Employee adherence to security policy and its effects	2
Top management support is critical for information security	5
Integration of technical and managerial activities for information security effectiveness	4
Information security should be dealt as a business issue	3
Security issues in cloud computing and management role	6
Security risk assessment and management role	6
Management role in security issues related to social media	2

Source: (Soomro et al., 2016)

1.2.4. Absence of Adequate Business – Cybersecurity Strategy

Strategy alignment is one of the main subject of enterprise architecture. Misalignment of business and IT strategy causes cybersecurity vulnerabilities. The interoperability and the partnership in the organization for cybersecurity management is important (Jalaliniya & Fakhredin, 2011: 27). Cybersecurity controls must align with the business area, the legal obligations, future needs and goals. Security functions

involve business processes and procedures. That's why business management and cybersecurity management must strike a balance to increase the business resilience and to create better business value.

1.2.5. Complexity in the Enterprise

Relatively large enterprises inevitably have complex structures with numerous dependencies. New business capabilities and growing IT landscapes with emerging technologies require more insight of the organization with its all assets and the relationships of these assets due to reduce the complexity. Enterprise architecture methodologies offers a layered perspective with business, application and infrastructure level (Landthaler, Kleehaus, & Matthes, 2016: 2).

1.2.6. Lack of Skilled Workforce

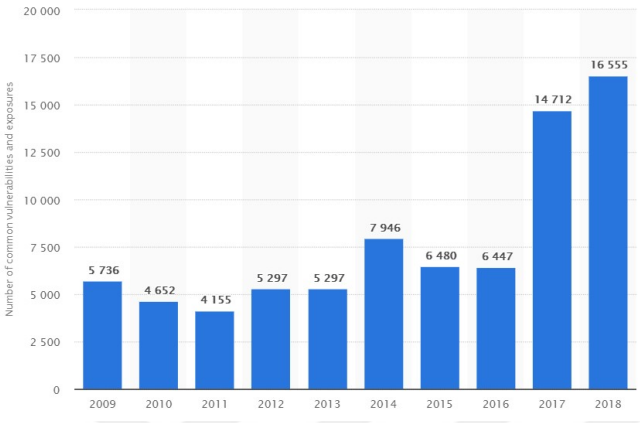
According to the report, employing the cybersecurity expert with the right skills is the major challenge for the enterprises (Schwab & Poujol, 2018: 10). Finding the right people and the right executives is very important to build cybersecurity workforce because the profession is relatively new in the field and finding experienced talents is difficult. As an example, in cyber incident response case business resilience requires talented individuals and if the organizations doesn't have this people, it is inevitable to establish strategic partnership with external solutions that have expertise in cybersecurity (Thompson, 2018: 4). These talented teams are formerly called computer incident response teams and computer emergency response teams. Today they called cybersecurity incident response teams.

1.2.7. Vulnerabilities That Increase Exponentially

Even the most robust systems have vulnerabilities and that's why the "zero days" exist. Zero-day attack is a type of cyberattack related to unknown vulnerabilities before. So vulnerability analysis with regular scans is very important for organizations.

In Fıgure 14, there is a report prepared by “cvedetails.com” and published by Statista, vulnerabilities that exposure are increasing.

Figure 14: IT Vulnerabilities Worldwide, 2009-2018



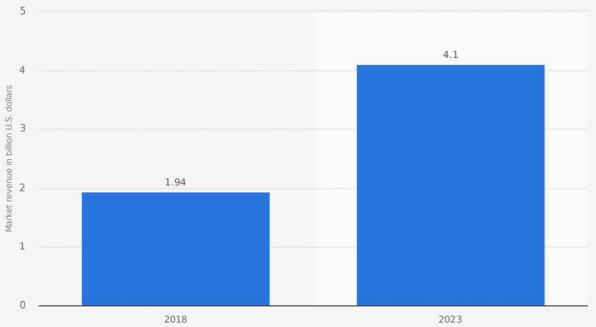
Source: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/ (03.07.2019)

1.3. THREATSCAPE FOR BUSINESSES

It is necessary to understand the threatscape that facing the organization and its systems. Vulnerabilities must be examined and it will be the integral part of first step of the cybersecurity strategy (Whitman, 2004: 44). In this chapter, several reports are referred and some of them overlaps. The reports show the most general sense of cyber threats to the businesses.

Denial of Service (DoS) attacks threatens business continuity directly. These attacks are increased in complexity and renamed as Distributed Denial of Service (DDoS) attacks. DoS /DDoS attacks can corrupt, interrupt or stop the business process or processes. Business resilience plan and cybersecurity management which involves the actions and procedures before, during and after a cyberattack is vital. In Figure 15, it is demonstrated that Denial of Service market expected to be doubled in five years.

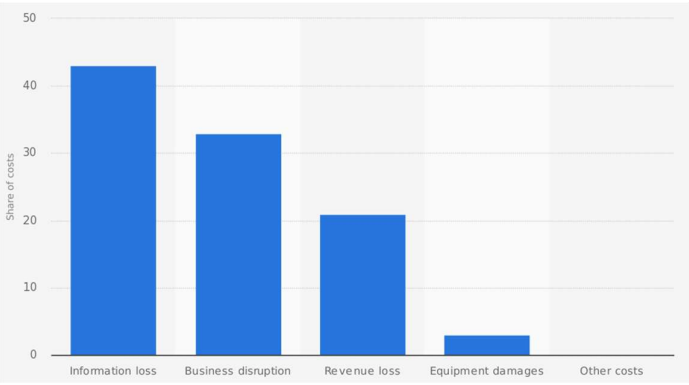
Figure 15: Forecast of Denial of Service Market, 2018-2023



Source: https://www.statista.com/statistics/985329/worldwide-ddos-protection-mitigation-market/ (20.04.2018)

Similar to previous threat, Figure 16 shows that business disruption is second costly incident. Data breaches and information leakage puts businesses in trouble due to regulations, prestige and customer and external parties trust, loss of revenue and productivity and forensic costs with the share of 43 percent of costs as a consequence of a cyberattack.

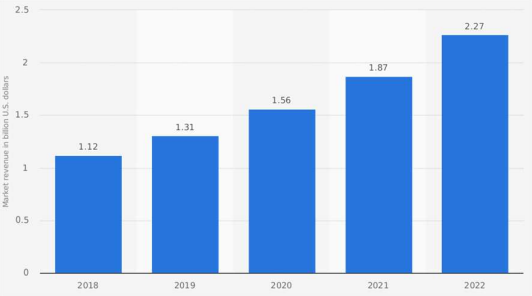
Figure 16: Costs of Cyberattacks Worldwide, 2017



Source: https://www.statista.com/statistics/241255/main-consequences-of-cyber-attacks-in-selected-countries/ (27.01.2019)

According to the Figure 17, the market of data loss prevention solutions is growing in future. Data Loss Prevention techniques generally address the endpoint security with remote management in the whole IT domain.

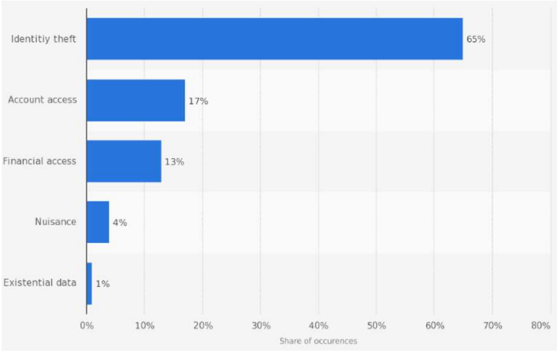
Figure 17: Data Loss Prevention Market Worldwide Forecast, 2018-2022



Source: https://www.statista.com/statistics/986319/worldwide-dlp-market-revenue-forecast/ (25.05.2019)

The human element is irreplaceable part of the cybersecurity management. Identity theft refers to authentication information, in other word usernames and password. These type of attacks easily steal the personal information via compromising e-mails and social media activities. Insider threat is another risk businesses faces due to dismissal of personnel, lack of belonging and blackmailing. According to Figure 18, Identity Theft share 65% of data breaches in occurrence frequency.

Figure 18: Data Breach Incident Types, Worldwide, 2018

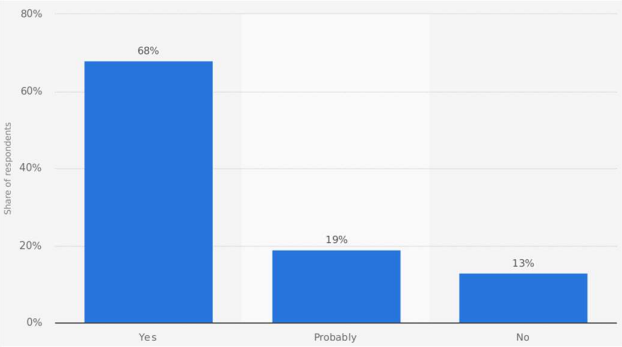


Source: https://www.statista.com/statistics/329593/frequency-share-incident-classifiaction-patterns/ (04.04.2019)

Cyber espionage is another risk caused by human element, generally caused by monetary reasons. Figure 19 depicts that, according to the survey conducted by Bitkom

Research, from 503 companies, 68% of them experienced cyber incident in terms of data theft, espionage and sabotage.

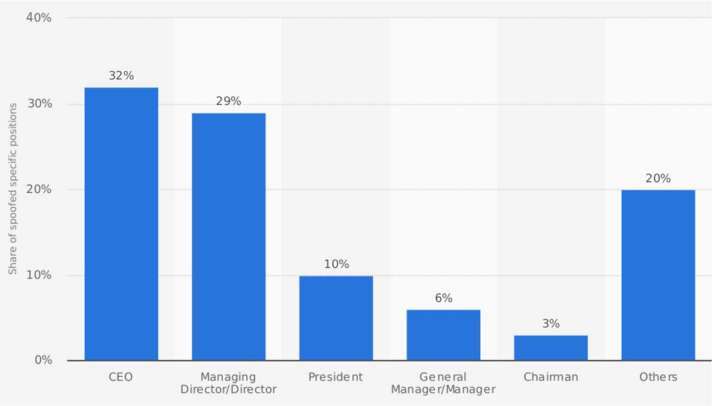
Figure 19: Data Theft, Espionage and Sabotage Incidents, Germany, 2018



Source: https://www.statista.com/statistics/429724/cyber-attacks-directed-at-companies-germany/ (29.01.2019)

Phishing and business e-mail compromise (BEC) is very common to organizations. Awareness activities plays an important role for improving basic information for employees. Figure 20 shows that top managers are commonly target of the business e-mail compromise attack.

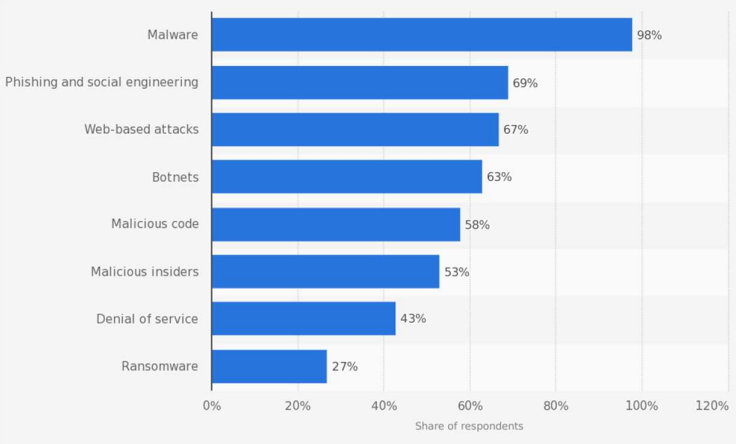
Figure 20: Business E-Mail Compromise Attacks Worldwide, 2018



Source: https://www.statista.com/statistics/820921/spoofed-specific-positions-attempts-by-bec-scams-fraud/ (01.04.2019)

Ransomwares and malwares also threatens the business endpoint security and the systems. Figure 21 shows that 98% of respondents in 254 companies worldwide experienced malware attacks in 2017.

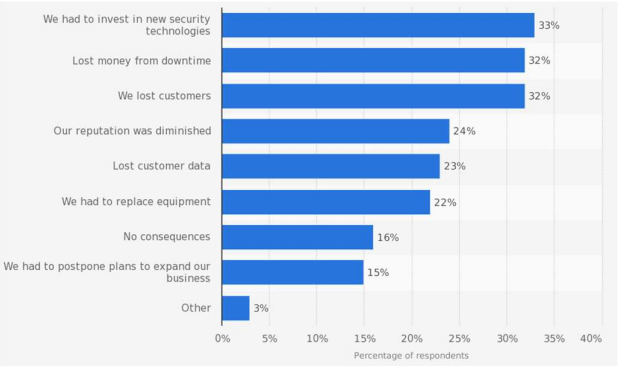
Figure 21: Types of Cyberattacks Worldwide, 2017



Source: https://www.statista.com/statistics/474937/cyber-crime-attacks-experienced-by-global-companies/ (27.01.2019)

Figure 22 depicts the most adverse effects of ransomwares such as investment in new technology, lost monetary, customer lost, reputation etc. for SME's in U.S. in 2016.

Figure 22: Consequences of Ransomwares Attacks, U.S., 2016



Source: https://www.statista.com/statistics/701287/consequences-of-the-ransomware-attack/ (01.04.2019)

Enterprises use content management systems. These systems are also under threat of cyberattacks. Physical Loss, theft, damage and the manipulation also concerns businesses.

CHAPTER TWO

CYBERSECURITY FOR BUSINESS RESILIENCE

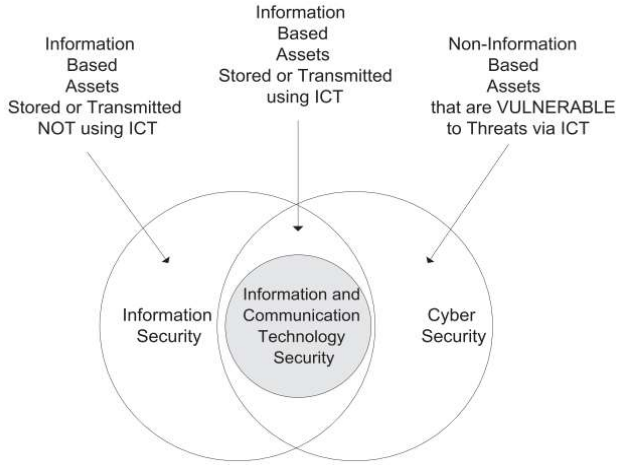
2.1. BUSINESS RESILIENCE

Resilience is an element of the trustworthiness including privacy, reliability and safety. Business resilience can be summarized as business fault tolerance and it refers to business continuity and organizational resilience with all business functions in case of any cyber incident. Recovery and improvement strategy is the main part of the business resilience (Abernathy & McMillan, 2018: 30). In case of a cyberattack, one or more asset can be adversely affected at the same time. Failure of an asset such as a device, a service or a whole system, can be a trigger for a new incident and solidary disruption can occur. In this situation, business impact analysis steps in. A comprehensive business resilience plan consists of cyber threat scenarios, asset dependencies, detection capabilities, recovery and back up procedures. In this manner digital business resilience is directly connected with cybersecurity. (*Insider Threat Program Guide*, 2019: 7).

2.2. CYBERSECURITY

Cybersecurity term is used alternately with computer security and information security but it is more beyond them. Cybersecurity involves the infrastructure, technologies, devices but also the processes and human element whom the significant part of it. Cybersecurity management consist of activities such as risk management, guidelines, best practices, training, etc. (Solms & Van Niekerk, 2013: 97) and functions which are studied in Chapter 2.3 “Defence in Depth Approach for Businesses”. Figure 23 illustrates the definitions. Cybersecurity is about all the ICT environment and involves both information based and non-information based assets. While information based assets are information itself in ICT based environment and related to directly information security, non-information based assets are technology based systems, where the information is processed, stored and transmitted.

Figure 23: Cybersecurity Definition



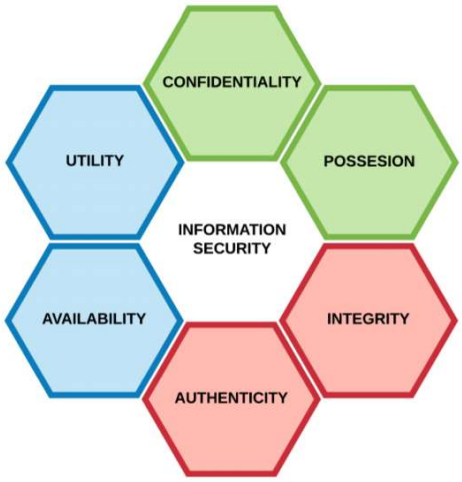
Source: (Solms et al. 2013: 101)

2.2.1. Information Security

The main purpose of ensuring information security is to avoid business disruption and lessen the adverse effects of any incidents (Solms, 1998: 224). Main aspects of information security are availability, integrity and confidentiality, this is called AIC Triad. Addition to this security framework, Donn B. Parker extends the model and add three more atomic elements in order to fill the gaps. The model called Parkerian Hexad, consists of confidentiality, integrity, availability, authenticity, possession / control and utility (Penber-Bey, 2012: 3).

Availability refers to access the data when needed. Loss of availability can cause business disruption and denial of service. Confidentiality refers to protect data from any unauthorized asset includes people and systems. Integrity refers to prevent the data from being changed out of the owners control in undesirable way. Authenticity refers proof of identity of the source of information. Possession or control is about ownership of the information and generally refers to pass in other hands. Utility refers to how useful data is and the state of quality and value of the data (Andress, 2014: 11). Figure 24 illustrates this framework.

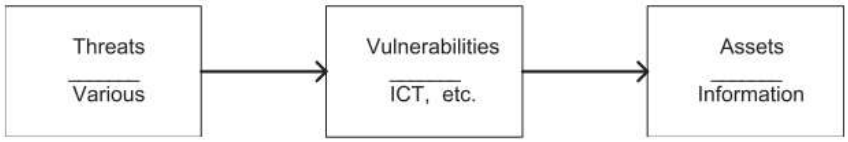
Figure 24: The Parkerian Hexad



Source: (Penber-Bey, 2012: 7)

Figure 25 presents the information security model. In this model, since the target asset is information, the cybersecurity risk is about threats to the vulnerabilities that information is processed, stored and transmitted environment has. Victim asset can a be computer, mobile phone, a file server, a sensor itself or a network, etc. In this case, the aim of the attacker is generally solely not to harm the ICT but to reach, leak and / or corrupt the main characteristics of information, mentioned in AIC triad or Parkerian Hexad so information needs protection. Composition of asset inventory and management, vulnerability analysis and threat assessment are main information security risk management activities.

Figure 25: Information Security Risk Model

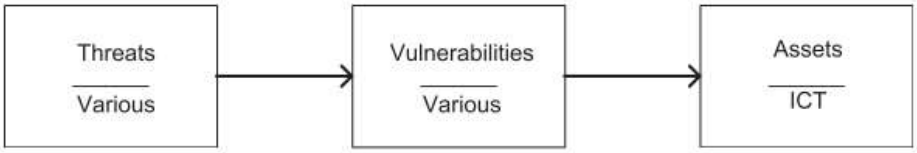


Source: (Solms & Van Niekerk, 2013: 99)

2.2.2. Information and Communications Technology (ICT) Security

ICT is the infrastructure of where information flows. When analysing information security, the asset that needs protection is information itself. But as presented in Figure 26, this time the asset needs to be protected is ICT itself. In this case, the attacker's intention is generally to harm the ICT infrastructure directly rather than to cause a data leak etc. Supervisory Control and Data Acquisition (SCADA) systems are generally victimised with this kind of incident (Solms & Van Niekerk, 2013:99).

Figure 26: ICT Security Risk Model



Source: (Solms & Van Niekerk, 2013: 99)

Information security, computer / network / ICT security, cybersecurity; these terms can be used interchangeably for anyone in the field but each of them separate areas, they often remind themselves, and strongly related to each other. Cybersecurity, is more involving as includes the whole assets one by one and the security domains by whole with all costs (Solms & Van Niekerk, 2013: 99).

2.3. DEFENSE IN DEPTH APPROACH FOR BUSINESSES

Cybersecurity risks turn out the business risks due to the dependency of digital technology that sets ground for nearly every business processes (The Open Group TOGAF-SABSA Integration Working Group, 2011: 4). In this case, not only the information or ICT but the whole business needs to be protected. Thus cyber resilience can almost reflect the business resilience which is mentioned previously.

In order to assure cyber resilience, several cybersecurity frameworks are developed by international organizations. Even the terms cybersecurity checklists / standards and frameworks are misused, the checklists and standards are mentioned

previously like ISO/IEC, NIST SP series, The CIS Security Controls for effective cyber defence and The Payment Card Industry Data Security Standard (PCI DSS) (Abernathy & McMillan, 2018: 35). The cybersecurity frameworks can be exemplified as National Institute of Science and Technology (NIST) cybersecurity framework (CSF) and Health Information Trust Alliance (HITRUST) CSF. There are also some other CSF initiatives but NIST CSF is the first to come to mind since being originally generated for critical infrastructures.

NIST CSF Framework for Improving Critical Infrastructure Cybersecurity is a comprehensive framework with main functions and the categories underneath the functions due to defence in depth approach. These cybersecurity functions are identification, protection, detection, response and recovery and they are discussed afterwards.

Enterprise architecture frameworks and methodologies can also be informative reference for these cybersecurity functions and this integration is studied in Chapter 3. All the functions are improved with former and current incidents so lessons learned programs and organizational communication plays an important role in cybersecurity frameworks.

2.3.1. Identification

Identification process involves people, process and technology. Identification phase is integral part of the business impact analysis. (Whitman, 2004: 43). According to the NIST Cybersecurity Framework, this phase consists of asset management, business environment, governance, risk assessment, risk management strategies including supply chain risk management.

Asset management category involves the inventory of all the ICT embers including physical devices and the systems, software and applications in the organization and information systems that are used outside of the organization are catalogued. Organization-wide data flow and communication maps are identified. All the assets such as resources, roles and all ICT members are classified in terms of business value and criticality due to impact analysis. In addition, cybersecurity roles

and the responsibility areas in the incident management teams and third party partners such as suppliers and customers are established.

Identification of business environment category identifies and priorities the organization's activities, missions, objectives and stakeholders for using it for risk management decisions.

In governance category, organizational cybersecurity requirements and policies such as operational, environmental, regulatory and legal are identified.

Risk assessment and risk management strategy including supply chain category focus on understanding the business risks, defining assumptions, priorities, constraints and risk tolerances for decision support (*Framework for Improving Critical Infrastructure Cybersecurity VER 1 1*, 2018: 7).

2.3.2. Protection

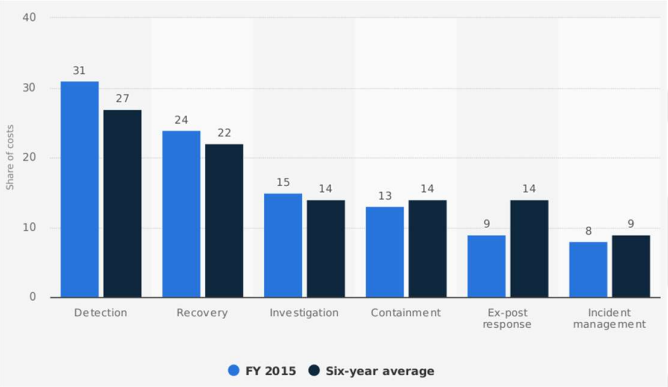
Protection function focuses on security policies that includes data security, and information protection addressing the roles, purposes, scopes and responsibilities among organizational assets and it subsumes protective technologies such as access control and identity management. Maintenance of the systems and awareness raising trainings are also under this category (Susanto & Almunawar, 2018: 143). Intrusion prevention systems (IPS), offers a proactive solution that avoids the possible victims from unwanted activities at network level.

2.3.3. Detection

Detecting the cybersecurity violations and the perpetrators of the violations is one of the hardest task and basically focus on monitoring and anomaly detection (Young & Windsor, 2010: 252). Security information and event monitoring (SIEM), and log management are fundamental detection activities (Poe, 2018: 95). There are also some intrusion detections systems (IDS) solutions that analyse the network traffic and use known indicators and security intelligence logged before, they also use machine learning and artificial intelligence to assess the normal state of the system due to anomaly detection (Thompson, 2018: 94).

Figure 27 shows the cyber incident related costs. According to the report, detection functions is the costliest activity. Recovery functions follows the detection in terms of costs and it is studied afterwards in this chapter. The rest of the activities summarizes the cybersecurity / business resilience activities mentioned before.

Figure 27: Cyber Incident Costs, U.S., 2015



Source: https://www.statista.com/statistics/250340/internal-costs-of-us-companies-due-to-cybercrime/ (14.09.2018)

2.3.4. Response

Incident response activity starts with detection of any suspicious event. Recent legal regulations such as GDPR force the businesses to change their incident response plans (Gavilan, 2016: 7). In response function, enterprise communication and response planning, incident analysis and mitigation processes are defined (*Framework for Improving Critical Infrastructure Cybersecurity VER 1 1*, 2018: 23). This function is also an important part of the business resilience. The response plans play a significant role during and after a cyber incident. The forensics and incident adversary impact analysis are done in this stage.

2.3.5. Recover

Recovery plans consist of backups, failsafe procedures, switching to reserve systems and restoration to a heathy point of the system. Similar to the incident response, recovery process is important due to business resilience and it is executed during and after a cyber incident. Other activities in this function are public relations and reputation management (*Framework for Improving Critical Infrastructure Cybersecurity VER 1 1*, 2018: 43). Enterprise communications again play an important role here (Sifaleras, 2019: 129).

CHAPTER THREE

ENTERPRISE ARCHITECTURE FOR INTEGRATED SECURITY

3.1. ENTERPRISE ARCHITECTURE FRAMEWORKS

An architecture is a fundamental of a system that conceptualizes the system's core properties such as its elements, the relationships of these elements and the design principles. To create a coherent, optimal complex system, such as an enterprise, a set of descriptive representations are needed. Architecture description serves also a baseline for change management of a system dealing with the complexity. An architecture framework is a practice of architecture description with creation, interpretation, analyse and usage. (Hinkelmann, 2012: 13).

Enterprise architecture is the blueprint that underlies the building blocks of the enterprise and it bonds mission, objectives, business processes and the ICT systems that enables the execution of these processes (Urbaczewski & Mrdalj, 2006: 18) and it gives a holistic view of the enterprise (Niemi, 2006: 1). Enterprise architecture relates the business and ICT department in business driven viewpoints (Janssen, 2009: 108). Enterprise architectures have some sub-architectures. These common sub-architectures are business, information, application, technology architecture. There are also some architecture views such as social, geospatial and security.

Holistic view of management, development of effective enterprise cybersecurity, proper management of IT infrastructure, business – human resources – IT alignment has a momentous impact of cybersecurity quality (Soomro et al., 2016: 215). It is generally shown the strategy triad as business, people and technology in literature. But recent studies emphasize the connections and relations, the harmony and the effectiveness of the system. Organisational business and IT values like resources of data and information can be protected by aligning cybersecurity management with business planning activities (Young & Windsor, 2010: 246). Multiple social and organizational factors must be combined to ensure effective cybersecurity management (Kayworth & Whitten, 2010: 1). One of the main cybersecurity challenges is while information and communications technology allows numerous of

business advantages, it causes to need also changes in organizational designs (Soomro et al., 2016: 215). Sometimes these organizations can be more complex. Within this scope, enterprise architecture can be beneficial for enterprise cybersecurity management.

The benefits attributable to enterprise architecture can categorized in hard benefits, intangible benefits, strategic benefits and indirect benefits. (Giaglis, Mylonopoulos, & Doukidis, 1999: 55). According to Niemi (2006:4) hard benefits are increasing interoperability, integration, standardization and reusability. Reducing costs and shortened cycle times can also be count in hard benefits of EA. Intangible benefits are holistic view of the enterprise, improved decision making and evolutionary governance and development. Strategic benefits are improved strategic agility, stability, communication and change management. Better business strategy – IT alignment is also one of the most important strategic benefit of EA. These benefits improves both operational capability and transformation capability (H. A. Proper & Lankhorst, 2014: 14).

On the other hand, there are some difficulties observed in using enterprise architecture methodologies and frameworks. Main struggles are the large variety of techniques and administrative skills are needed to manage the information and variety of models gathered from cross references (Promis, Ag, & McLeod, 2008: 1). This situation reflects the importance of enterprise architect role and enterprise architecture board in the organization.

3.1.1. The Zachman Framework for Enterprise Architecture

The Zachman Framework for enterprise architecture visualises the enterprise at one glance and is an intellectual tool that describes the complex organizations (Mowbray, 2014: 5) consisting two-dimension matrix and the rows represent five “W” questions (What, Where, Who, When, Why) and a “How” question. The columns represent the roles in the enterprise with management layers such as executives, business managers, architects, engineers, technicians and the whole enterprise itself (Zachman, 1987: 276). This framework does not formally define the processes (Aier et al., 2010: 12). The Zachman Framework tend to be useful for cybersecurity risk

management by enabling the visibility in the enterprise (Mowbray, 2014: 37). There are some Zachman-based security architecture frameworks such as Henning (1996), DeLooze (2001) and Heaney (2003). Heaney adds a new column to the matrix and names as Information Assurance (IA). DeLooze stresses the importance data access control and groups the enterprise data such as employee data, customer data, etc. (Jalaliniya & Fakhredin, 2011: 35)

3.1.2. Department of Defence Architecture Framework (DoDAF)

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Architecture Framework (C4ISRAF) developed by Department of Defense, US in 1996 which is influenced by The Zachman Framework for Enterprise Architecture. And it is replaced with Department of Defence Architecture Framework (DoDAF) in 2003 (McDowall, 2019: 4). It is first seen in public sectors and it approaches to the enterprise architecture with several viewpoints in capability, operational, data and information, operation, projects, services, standards and systems (Abernathy & McMillan, 2018: 10). Data views are consist of conceptual, logical and physical (Mayer, Aubert, Grandry, & Feltus, 2016: 6).

3.1.3. The Open Group Architecture Framework (TOGAF)

TOGAF is first introduced by The Open Group which is a consortium, in 1998 and is also influenced by Zachman Framework (McDowall, 2019: 4). TOGAF approach has different architecture domains: business architecture, data architecture and application architecture. Having the feature of architecture development method, TOGAF can integrate any other methodologies like ITIL or any other legacy procedures.

In the architecture development method of TOGAF, preliminary face is followed with architecture vision, business architecture, information systems architectures, technology architecture, opportunities and solutions, migration planning, implementation and governance, architecture change management steps. All

these steps related with the requirements management (The Open Group TOGAF-SABSA Integration Working Group, 2011: 9).

The content metamodel of TOGAF elaborates the architecture vision with business strategy, technology strategy, business principles, objectives, drivers and stakeholders. Business architecture is expanded with motivation, organizational units, locations, actors, roles and functions such as business services, processes, events, controls and products. Information systems architecture is sliced in two, data and application components with physical and logical environment. Technology architecture consists physical and logical components, platforms and services. Architecture realization presents opportunities, solutions, migration and governance, including standards, guidelines and specifications (The Open Group TOGAF-SABSA Integration Working Group, 2011: 10).

3.2. RELATED METHODOLOGIES

While methodology is a systematic set of methods and body of rules and principles with a base of knowledge in the field of study, framework is a functional collection which is an abstraction and flexible to selective changes based on the business cases. Methodology is more specific and includes detailed information rather than frameworks.

3.2.1. Sherwood Applied Business Security Architecture (SABSA)

SABSA is similar to the Zachman Framework with six horizontal layers (contextual, conceptual, logical, physical, component and service) and vertical layers with the same questions with the Zachman Framework for enterprise architecture: what for assets, why for motivation, how for process and technology, who for people, where for location and when for time or time to market (Sherwood, Clark, & Lynas, 2009: 8) SABSA methodology differ than an architecture framework with its management matrix, business attributes, governance and risk management models (Sherwood et al., 2009: 24).

3.2.2. Control Objectives for Information and Related Technology (COBIT)

COBIT is developed by a non-profit organization called Information Systems Audit and Control (ISACA). The main characteristics of the framework is meeting needs of stakeholders, cover enterprise as a whole, it is a single framework itself consists principles, policies and frameworks (Abernathy & McMillan, 2018: 12).

3.2.3. Information Technology Infrastructure Library (ITIL)

ITIL itself is not an enterprise architecture methodology but it supports that IT service strategy should align with the business strategy. ITIL adds effectiveness and efficiency with focusing of the IT service management lifecycle. ITIL service strategy consist of configuration management, event management, availability management and incident management (Sigler, 2018: 264).

CHAPTER FOUR

EVALUATION OF ENTERPRISE ARHITECTURE AND CYBERSECURITY MANAGEMENT REALTIONSHIP

4.1. STUDY

This is a qualitative study consisting of questionnaires and interviews. The main purpose of this study is to reveal the relationship between enterprise architecture methodologies and cyber security management by gathering experiences and opinions about key issues in the field.

Elite interviews are conducted with executives and professionals in the expertise of cybersecurity and enterprise architecture, one is from a large international organization and the other five is from Turkey's large and significant enterprises between December 2018 and April 2019.

Research surveys are conducted with business executives, technical experts and white collar employees as a part of IT domain.

4.1.1. Objective of the Study

This literature review shows that IT and cybersecurity professionals cannot safe the organizations from the adverse effects of cyber incidents due to business continuity and other concerns without organizational support and involvement, including both business managers, employees, etc. On the other side, while management deals with non-technical aspects of cybersecurity, risk management is too hard to accomplish for the executives without technical support. It can be concluded that technical and managerial activities must be well integrated and aligned (Singh, Picot, Kranz, Gupta, & Ojha, 2013: 226; Soomro et al., 2016: 220; Young & Windsor, 2010). But many organizations experience that cybersecurity solutions are heavily on technical basis, unfortunately, separate from organizational business strategy and business processes (The Open Group TOGAF-SABSA Integration Working Group, 2011). This study primarily focusses on the possible collaborative force of enterprise

/ business architecture methodologies and cybersecurity management frameworks for better cybersecurity posture for the organizations adverted in Chapter 3.

There are also sub-objectives of this research;

- To observe the awareness of the cybersecurity and cyber defence, the business concerns, the struggles of managing risks, the threatscape and the success factors referred in Chapter 1 and Chapter 2, Cybersecurity for Businesses and Defence in Depth Approach in terms of Business Resilience.
- To determine whether there are any dependencies between cybersecurity management and business management in strategic, operational and tactical level mentioned in Chapter 3.
- To investigate the possible effects of interoperability of enterprise architecture methodologies and cybersecurity management frameworks adverted in Chapter 3.

4.1.2. Data Collection Method

The unstructured interviews are conducted with the professionals and top executives towards enterprise architecture, cybersecurity and business management fields to gain deeper insights to support for both setting the framework of the study and to make contribution to the findings. The interviews are carried out face to face and by online video calls (Zoom Interview Application). Each of these interviews lasted from one hour to one and a half hours. Some interviews are repeated due to consolidation and knowledge sharing. As a consequence of all interviews, it is expressed by the interviewees that they are pleased to contribute the research and they are satisfied with the interview framework. They also think that the objective of the study contributes with the cybersecurity and business field in a serviceable manner.

Due to preparation for research surveys, literature review and a pilot study has applied to field professionals, white-collar employees, executives and academicians to test the comprehensibility of the questions in the survey. The survey is finalized with the feedbacks collected from pilot respondents mentioned above. Even some questions are explanatory, a brief explanation have been made orally and text-based to each

respondent when needed. After the briefing, it is expressed by the respondents that the baseline information is needed for the survey. The surveys conducted by face to face and online Google Forms. Most of the data collected by online forms with the intention of reach as much as chosen, relevant respondents.

The research survey is constructed consists of three main parts with questions. The first part includes three demographic questions such as job roles, enterprise levels and sectors. In the second part, the knowledge level of cybersecurity based business risks and the awareness of adverse effects those related to consequences of cyber incidents and the general opinion of cybersecurity management are observed. The third and the last section discussed enterprise architecture driven cybersecurity.

Likert Scale has been chosen to apply for the surveys, based on the scale of the responses from strongly disagree (1) to strongly agree (5). The survey ends with open ended questions to gather any additional data, custom opinions and feedbacks.

4.1.3. Sampling

In elite interviews, non-probability sampling method is used. Due to being a clear focus for cases but also difficult to reach, critical case purposive and volunteer sampling is conducted (Saunders, Lewis, & Thornhill, 2012: 283). Six interviewees consist of one operational excellence executive officer, two enterprise architecture executives and three cybersecurity executives from large enterprises.

Purposive and volunteer samplings techniques are used in the sampling method. The target group consist of business executives, IT consumers such as process owners and white collar employee, ICT / Cybersecurity managers and professionals mostly in large enterprises in both private and public sectors. The sample size of the study is 125. Survey participant size is one of the most important limitation of the study and is discussed further in Section 4.1.5.

4.1.4. Data Analysis

In unstructured interviews, content analysis technique is used. Keywords are enterprise architecture methodologies, benefits, struggles, impact analysis, relation and collaboration of cybersecurity and enterprise architecture, strategy alignment and cybersecurity management derived from this literature. Interview questions are placed in Appendix 1.

In the in-depth interviews,

Question 1. evaluates the familiarity levels of executives with enterprise architectures and the distribution of enterprise architectures.

Question 2. evaluates the possible benefits of enterprise architecture in the organization.

Question 3. evaluates main problems in managing cybersecurity risk in the organization.

Question 4. evaluates the maturity levels of analysing business impacts in case of a cyber incident.

Question 5. evaluates the perception of how cybersecurity risks put business into risks.

Question 6. evaluates the application of strategy alignment between IT – Cybersecurity and business strategy.

Question 7. evaluates how serviceable is collaboration between enterpeise architecture and cybersecurity management.

Question 8. asks for any contribution to the idea of better cybersecurity management.

Research survey, placed in Appendix 2. consists of 35 questions. First five question asks for the descriptive information such as name, surname, job role in the organization, enterprise level and sector. following part of the survey consists of four questions that evaluates the awareness of the severity of a cyber incident in the organization. Third part of the survey consists of cybersecurity and cybersecurity strategy related questions. This part of the survey consists of 13 questions and evaluates the perception of the responsibility are of cybersecurity management in the organization and how cybersecurity strategy has to be aligned and shaped. The main

significant factors are also asked to the respondents in this part of the survey. Fourth part consists of nine questions related enterprise architecture and evaluates the distribution of enterprise architectures and how enterprise architecture can be beneficial in better cybersecurity. Fifth and the last part of the survey consists of four open ended questions. These questions are asked about additional feedback relating cybersecurity management and enterprise architecture and also the satisfaction and the recommendations of the survey.

To analyse the data which collected from research survey, IBM SPSS Version 24, a statistics software is used and also benefited from Google Forms. Reliability test, descriptive statistics and linear modelling are conducted on SPSS program.

4.1.5. Limitations of the Study

The limitations of the study can be categorised in two: content and participant size.

In the sense of content, the organizational measures of cybersecurity such as programs, procedures and control checklists are confidential virtually for all respondents so that they avoid sharing these kind of information. They also pleased in order not to share any personal or corporate information.

With regard to participant size, due to cybersecurity is a business critical function, the executives and other professionals refrain from participating the surveys and giving any information not only about their organizations but also personal opinions in terms of legal obligations and they beware revealing the maturity level and exposing the possible vulnerabilities of the organizations for both sectors and almost for all enterprise levels. The other limitation about sampling size is the skill shortage. It is not quite easy to find an expert in the field to discuss the study due to the talent gap in the industry. Lastly, even the cybersecurity is a multidisciplinary profession beyond ICT and almost everyone has a bit of opinion in social lives and at work places, the people choose to stand clear, possibly caused by lack of self-confidence about the subject.

4.2. FINDING

In the interviews, respondents are asked to share their view of points about collaboration of enterprise architecture methodologies and cybersecurity management.

Cybersecurity experts emphasize the idea of “security from scratch” because it is experienced that security is sometimes an afterthought subject. Another enterprise architecture serviceableness they expressed that better capability to layered security in the organization, creating common language and point of view organization wide. They agreed that better prioritization, better planning and better strategic alignment are advantages of the enterprise architectures. On the other hand, apart from methodologies, they expressed that the most important struggle they recently experience is lack of talent and cybersecurity workforce.

Enterprise architecture executives see the cybersecurity management activities in strategy, business, application, data and technology level. They express that enterprise architecture may change the out of date managerial habits to manage today’s and tomorrow’s risks. They take analysis as looking at the mirror for the enterprises so that provides seeing the big picture with its pros and cons. They stated that they use some tools (like Alphabet) to manage the enterprise architecture activities for example tracking projects and they take the advantage of avoid unnecessary resource utilization in terms of business and IT alignment.

4.2.1. Reliability of the Scales

In the research survey, Likert-type scales are mostly used. Therewith for the reliability of the scales, Cronbach’s alpha value is reported. In order to be considered reliable for analyses, alpha value threshold is 0,70 for reflective measurement models (Nunnally, 1978). Table 2 indicates that scales used in this study is reliable.

Table 2: Reliability Analysis

Constructs	**Cronbach's Alpha Value**
Overall	.844
Awareness of Relation of Cyber Risks and Business Risks	.789
Attitude Towards Business Driven Approach	.725
Perceived Advantage of Alignment	.830

4.2.2. Demographics Characteristics of the Sample

The frequency distribution of job roles, enterprise levels, sectors enterprise architecture usage, methodology framework and preferences, and participants' feedback of research survey are indicated in the following tables and figures.

Table 3 demonstrates 125 people who responds to the questionnaire and their job roles. 55% of respondents are technical personnel and 45% of respondents are business owners and consumers of information systems in the organization.

Table 3: Descriptive Statistics of Job Role

Job Role	**N**	**Percentage**
IT Manager	23	18.4
ICT Specialist	23	18.4
Executive Manager	19	15.2
InfoSec / Cybersecurity Manager	10	8.0
Software Developer	9	7.2
Project Manager	8	6.4
Enterprise Architect	5	4.0
InfoSec / Cybersecurity Specialist	3	2.4
Other	25	20.0
Total:	**125**	**100.0**

Table 4 shows the organization size by number of employees. The majority of respondents of research survey works in relatively large enterprises. The large enterprises are known that they are able to leverage the technology due to creativity and business value but on the other hand they have to deal with complexity in terms of governance (Bloomberg & Schmelzer, 2013).

Table 4: Descriptive Statistics of Enterprise Level

Number of Employees	**N**	**Percentage**
More than 250	63	50.4
50-249	34	27.2
10-49	15	12.0
Less than 10	13	10.4
Total:	**125**	**100.0**

Table 5 indicates the share of the sectors that respondents work. In research survey, it is tried to include both sectors as equal as possible with the purpose of more inclusive and extensive research.

Table 5: Descriptive Statistics of Sector

Sector	**N**	**Percentage**
Private	74	59.2
Public	51	40.8
Total:	**125**	**100.0**

Table 6 shows enterprise architecture usage among respondents. 43,2% of respondents express the organizations they work has an enterprise architecture methodology and 28% of the rest plans to adopt and/or adapt an enterprise architecture in future. Nearly every one of three respondent declares that they have no any enterprise architecture application in their organizations and 13,6% of respondents have never heard of such a methodology ever.

Table 6: Enterprise Architecture Usage

Enterprise Architecture Methodologies Usage	**N**	**Percentage**
Enterprise architecture methodology is applied.	54	43.2
It is planned to adopt / adapt an enterprise architecture methodology in the future.	35	28.0
There is no enterprise architecture practice and it is not planned in near future.	17	15.2
I've never heard of enterprise architecture before, I learned it through this survey.	19	13.6
Total:	**125**	**100.0**

When participants are asked to select the preference of the enterprise architecture methodology and / or framework in the multiple choice question, while 70 of the participants selected at least one enterprise architecture and some of them chose multiple enterprise architectures; rest of them, which means 55 of the participants chose not to respond any enterprise architecture. Due to analyse multiple responses, the frequency, the percentage and the percent of the cases of enterprise architectures are calculated and the responses are normalized by 100 percent. The percentage of case's value is more than 100 because of multiple choices. Table 7 indicates that TOGAF Enterprise Architecture takes most of the share by 46,5% in enterprise architecture methodologies among respondents' preferences. One reason for that may Architecture Development Method of TOGAF can include any other methodologies inside at Architecture Vision as mentioned in detail at Chapter 3. Similarly, a survey (Carr & Else, 2018) conducted in 2018 with 19 participant countries, it is reported that TOGAF is used mostly for the reason of trainings and certification programs given by The Open Group, owners of TOGAF. ITIL also has a big share on the second seat with 39,40%. As mentioned in Chapter 3, ITIL specifies the general framework between IT department or service provider and customer or whole organization. That's why it is commonly used. In preferences, other means, some organizations apply their custom minimal architecture methodologies.

Table 7: Methodology and Framework Preferences

Enterprise Architecture Methodology / Business Framework	**N**	**Percentage**	**Percent of Cases**
TOGAF	46	46.5	65.7
ITIL	39	39.4	55.7
Other	7	7.1	10.0
COBIT	3	3.0	4.3
SABSA	3	3.0	4.3
The Zachman Framework	1	1.0	1.4
Total:	**99**	**100.0**	**141.4**

4.2.3. Descriptive Statistics

According to the descriptive statistics shown in Table n, the perception of cyber incidents in terms of businesses risk is significant with the average mean value of 4.5. Results indicate that business continuity is the top concern for participants in cybersecurity related risks. Most of the respondents think that cybersecurity is not only IT personnel's but also business owners' and top managers' responsibility.

It is commonly agreed that cybersecurity strategy should involve all the functions (identify, protect, detect, response, recover) by means of identifying the business processes, connections of the business processes (as an asset) with business driven approach. They also agree that legal obligations can affect cybersecurity strategy. The importance of cybersecurity awareness is the point where nearly everyone strongly agrees with the mean value of 4.61.

According to the research survey responses, social and behavioural factors like human element, communications and managerial habits also have a significant effect in cybersecurity. It is shown that the participants don't come to a common point about perception of the cybersecurity as just firewalls and antiviruses. While some participants believe that cybersecurity has taken into just technical subject, the others think that it is more than that.

In the perceived benefits of enterprise architecture methodologies for cybersecurity management partition, the most prominent function is business risk assessment. Participants believe that enterprise architecture is a solution for risk assessment and asset management activities. It is widely perceived that enterprise architecture driven cybersecurity approach may increase situational awareness in the enterprise by reducing complexity. Mentioned approach may provide convenience for prioritisation in practice and for better investment decisions by reducing costs.

Table 8: Descriptive Statistics

	N	Mean	Standard Deviation	Min	Max
Perceived Cyber Risks (PCR)		**4.5013**			
Business Continuity	125	4.5600	0.70023	2.00	5.00
Serious Losses	125	4.5280	0.70225	2.00	5.00
Service Dependency	125	4.4160	0.82486	1.00	5.00
Perceived Responsibility (PR)		**4.3040**			
Process Owner Responsibility	125	4.3040	0.75374	2.00	5.00
Top Management Responsibility	125	4.3040	0.77485	2.00	5.00
Perceived Cybersecurity Strategy (PCS)		**4.2547**			
Cybersecurity Functions	125	4.4960	0.67947	2.00	5.00
Asset Relations	125	4.4080	0.74158	2.00	5.00
Business Processes	125	4.2560	0.77151	1.00	5.00
Business Area	125	4.2400	0.77668	1.00	5.00
Business Driven	125	4.0800	0.91228	1.00	5.00
Legal Obligations	125	4.0480	1.02277	1.00	5.00
Perceived Cybersecurity in General (PCG)		**4.2800**			
Cybersecurity Awareness	125	4.6160	0.57899	3.00	5.00
Human Factor	125	4.5600	0.66478	2.00	5.00
Communications	125	4.5520	0.71229	2.00	5.00
Management Habits	125	4.3120	0.72308	2.00	5.00
Hardware and Software	125	3.3600	1.33441	1.00	5.00
Perceived Benefits of Enterprise Architecture for Cybersecurity (PBEAC)		**4.2914**			
Impact Analysis	125	4.4400	0.64006	3.00	5.00
Asset Management	125	4.3440	0.68514	3.00	5.00
Situational Awareness	125	4.3360	0.63429	3.00	5.00
Strategy Alignment	125	4.2960	0.68420	3.00	5.00
Investment Decisions	125	4.2560	0.77151	2.00	5.00
Prioritize	125	4.2400	0.77668	1.00	5.00
Complexity	125	4.1280	0.93305	1.00	5.00

Table 9 indicates that cybersecurity is a prestigious subject virtually for all organizations and besides external stakeholders are generally not taken into account for both public and private sectors. According to the public sector participants, revenue

is one of the least important concerns about cyber incidents. Response and recovery effort and external stakeholders have the same share for public sector. When it comes to private sector, the most important concern is revenue and prestige follows it.

Table 9: Perceived Adverse Effects of Cyber Incidents

Overall		
Adverse Effects	**Percent**	**Percent of Cases**
Prestige	22.9	78.9
Revenue	21.5	74.0
Consequences of regulatory requirements	21.0	72.4
Effort	19.1	65.9
External Stakeholders	15.6	53.7
Total:	**100.0**	**344.7**
Public Sector		
Adverse Effects	**Percent of Cases**	
Prestige	78.4	
Consequences of Regulatory Requirements	66.7	
Effort	60.8	
External Stakeholders	60.8	
Revenue	60.8	
Private Sector		
Adverse Effects	**Percent of Cases**	
Revenue	83.3	
Prestige	79.2	
Consequences of Regulatory Requirements	76.4	
Effort	69.4	
External Stakeholders	48.6	

Table 10 shows the perception of the direct responsibility of cybersecurity in an organization. Cybersecurity experts and managers, and enterprise architects in respondents tend to share the responsibility with the executive board directly in the organization due to business driven approach with smaller standard deviation. On the other hand, with bigger standard deviation, some executive managers seem that they want to be a little bit far from the responsibility area and project managers are also fragmented about perception about the responsibility. In personal interviews, it is reported that the responsibility is left to cybersecurity expert roles since it is a technical

issue. But overall perception shows that every role in the IT domain in the organization relatively agree that cybersecurity activities need executive support and cybersecurity management responsibility is directly related with the top management.

Table 10: Top Management Responsibility of Cybersecurity

Job Role	N	Mean	Standard Deviation
InfoSec / Cybersecurity Specialist	3	5.00	0.00
InfoSec / Cybersecurity Manager	10	4.20	0.42
Enterprise Architect	5	4.20	0.45
ICT Specialist	23	4.43	0.73
IT Manager	23	4.26	0.75
Software Developer	9	4.22	0.83
Other	25	4.24	0.88
Executive Manager	19	4.37	0.90
Project Manager	8	4.13	0.99

Table 11 shows the group statistics about the difference of perceptions between technical personnel and business executives. According to the statistical results, the perception of extra effort caused by a cyber incident, the importance of cybersecurity awareness, enterprise architecture's positive effect on cybersecurity and business strategies alignment, and possible advantages of enterprise architecture about cybersecurity investment decisions are significant different in two groups: technical personnel and business executives.

According to Table 11, technical personnel concern more about extra effort caused by a cyber incident compared to business executives. Business executives pays more attention to cybersecurity awareness among the organization. Respondents who has technical background are closer to the idea that enterprise architecture provides better business strategy and cybersecurity strategy alignment and better investment decisions.

According to the survey findings shown in Table 11, even technical personnel seem to closer the idea that cybersecurity activities should be business driven, human factor is important in cybersecurity, enterprise architecture reduces complexity in cybersecurity management and enterprise architecture provides better prioritization, there is no significant difference statistically with the other group, business executives.

Table 11: T-Test Group Statistics: Perception by Proficiency

Perceptions	Groups	N	Mean	Std. Deviation	t	df	P
Effort	Techie	46	3,4348	0,58318	2,070	82	**0,042**
	Business	38	3,1842	0,51230			
Cybersecurity Awareness	Techie	68	4,5147	0,63464			
	Business	57	4,7368	0,48279	-2,168	123	**0,032**
Strategy Alignment	Techie	68	4,4412	0,60797	2,610	108,875	**0,010**
	Business	57	4,1228	0,73364			
Investment Decisions	Techie	68	4,4559	0,67876	3,235	109,381	**0,002**
	Business	57	4,0175	0,81265			
Business Driven	Techie	68	4,2059	0,82061	1,668	108,401	0,098
	Business	57	3,9298	0,99749			
Human Factor	Techie	68	4,6324	0,62065	1,318	112,250	0,19
	Business	57	4,4737	0,70976			
Complexity	Techie	68	4,2500	0,79879	1,568	102,543	0,12
	Business	57	3,9825	1,06051			
Prioritize	Techie	68	4,3088	0,65237	1,053	99,821	0,295
	Business	57	4,1579	0,90217			

In Table 12, t-test, is a type of inferential statistics is applied. Two tailed p-value (< 0,05) shows that there is a significant difference between the means of two groups (business and technical personnel) about perceptions those mentioned above in Table 11: effort, cybersecurity awareness, strategy alignment and investment decisions. “Supported” at Test Results tab shows the significant different ones.

Table 12: T-Test Independent Samples

		Levene's Test for Equality of Variances		t-test for Equality of Means					
Perceptions	**Equal Variances**	**F**	**Sig.**	**t**	**df**	**Sig. (2-tailed)**	**Mean Differen**	**Std. Error**	**Test Results**
Consequences of regulatory requirements	Assumed	0,528	0,469	-0,401	121	0,689	-0,06130	0,15269	Not supported
	Not Assumed			-0,397	111,537	0,692	-0,06130	0,15423	
Prestige	Assumed	1,339	0,250	-0,236	107	0,814	-0,04235	0,17970	Not supported
	Not Assumed			-0,233	95,544	0,816	-0,04235	0,18200	
Effort	Assumed	9,079	0,003	2,070	82	**0,042**	0,25057	0,12108	**Supported**
	Not Assumed			2,095	81,667	0,039	0,25057	0,11958	
Revenue	Assumed	1,584	0,213	0,626	59	0,534	0,05195	0,08299	Not supported
	Not Assumed			0,616	52,219	0,541	0,05195	0,08437	
Business Continuity	Assumed	0,393	0,532	-1,047	123	0,297	-0,13158	0,12570	Not supported
	Not Assumed			-1,047	119,452	0,297	-0,13158	0,12564	
Service Dependency	Assumed	0,691	0,407	-0,062	123	0,950	-0,00929	0,14873	Not supported
	Not Assumed			-0,061	106,383	0,951	-0,00929	0,15169	
Serious Losses	Assumed	0,002	0,962	0,024	123	0,981	0,00310	0,12662	Not supported
	Not Assumed			0,024	118,704	0,981	0,00310	0,12676	
Top Mgmt Responsibility	Assumed	1,073	0,302	0,538	123	0,592	0,07508	0,13955	Not supported
	Not Assumed			0,529	108,381	0,598	0,07508	0,14196	
Process Owner Responsibility	Assumed	1,000	0,319	0,078	123	0,938	0,01058	0,13590	Not supported
	Not Assumed			0,077	113,699	0,939	0,01058	0,13723	
Business Area	Assumed	1,163	0,283	-0,304	123	0,762	-0,04257	0,13999	Not supported
	Not Assumed			-0,302	115,311	0,763	-0,04257	0,14100	
Legal Obligations	Assumed	3,203	0,076	0,129	123	0,898	0,02374	0,18440	Not supported
	Not Assumed			0,126	108,133	0,900	0,02374	0,18765	
Business Processes	Assumed	0,844	0,360	0,369	123	0,713	0,05134	0,13903	Not supported
	Not Assumed			0,364	109,644	0,717	0,05134	0,14120	
Business Driven	Assumed	1,708	0,194	1,698	123	0,092	0,27606	0,16260	Not supported
	Not Assumed			1,669	108,402	0,098	0,27606	0,16541	
Cybersecurity Functions	Assumed	0,611	0,436	-0,192	123	0,848	-0,02348	0,12250	Not supported
	Not Assumed			-0,189	111,483	0,850	-0,02348	0,12409	
Asset Relations	Assumed	0,006	0,937	-0,421	123	0,675	-0,05624	0,13362	Not supported
	Not Assumed			-0,424	122,028	0,672	-0,05624	0,13257	
Hardware and Software	Assumed	0,052	0,821	1,148	123	0,253	0,27477	0,23933	Not supported
	Not Assumed			1,148	119,212	0,253	0,27477	0,23933	
Mgmt Habits	Assumed	1,647	0,202	0,939	123	0,349	0,12203	0,12991	Not supported
	Not Assumed			0,921	106,345	0,359	0,12203	0,13251	

Table 12: T-Test Independent Samples (Continued)

		Levene's Test for Equality of Variances		t-test for Equality of Means					
Perceptions	**Equal Variances**	**F**	**Sig.**	**t**	**df**	**Sig. (2-tailed)**	**Mean Differen**	**Std. Error**	**Test Results**
Cybersecurity Awareness	Assumed	12,978	0,000	-2,168	123	**0,032**	-0,22214	0,10246	**Supported**
	Not Assumed			-2,220	121,920	0,028	-0,22214	0,10006	
Communications	Assumed	1,594	0,209	-0,638	123	0,525	-0,08179	0,12822	Not supported
	Not Assumed			-0,651	122,700	0,516	-0,08179	0,12570	
Human Factor	Assumed	2,555	0,112	1,333	123	0,185	0,15867	0,11901	Not supported
	Not Assumed			1,318	112,250	0,190	0,15867	0,12043	
Strategy Alignment	Assumed	0,181	0,671	2,653	123	0,009	0,31837	0,11998	
	Not Assumed			2,610	108,875	**0,010**	0,31837	0,12198	**Supported**
Asset Mgmt	Assumed	0,272	0,603	0,420	123	0,675	0,05186	0,12345	Not supported
	Not Assumed			0,418	116,225	0,677	0,05186	0,12415	
Complexity	Assumed	2,415	0,123	1,607	123	0,111	0,26754	0,16650	Not supported
	Not Assumed			1,568	102,543	0,120	0,26754	0,17063	
Situational Awareness	Assumed	1,010	0,317	0,608	123	0,544	0,06940	0,11420	Not supported
	Not Assumed			0,601	112,360	0,549	0,06940	0,11554	
Prioritize	Assumed	3,192	0,076	1,083	123	0,281	0,15093	0,13938	Not supported
	Not Assumed			1,053	99,821	0,295	0,15093	0,14331	
Impact Analysis	Assumed	0,076	0,783	0,302	123	0,763	0,03483	0,11537	Not supported
	Not Assumed			0,301	117,853	0,764	0,03483	0,11569	
Investment Decisions	Assumed	0,770	0,382	3,286	123	0,001	0,43834	0,13338	
	Not Assumed			3,235	109,381	**0,002**	0,43834	0,13550	**Supported**

According to the linear modeling, Figure 28 shows that the responses given about business driven approach in cybersecurity is the most important predictor of business cybersecurity strategy alignment. That means, who declares cybersecurity strategy should be business oriented also thinks that business strategy and cybersecurity strategy should be aligned. Identification of business area and business processes are shown in terms of prediction importance in strategy alignment.

Figure 28: Predictors of Business - Cybersecurity Strategy Alignment

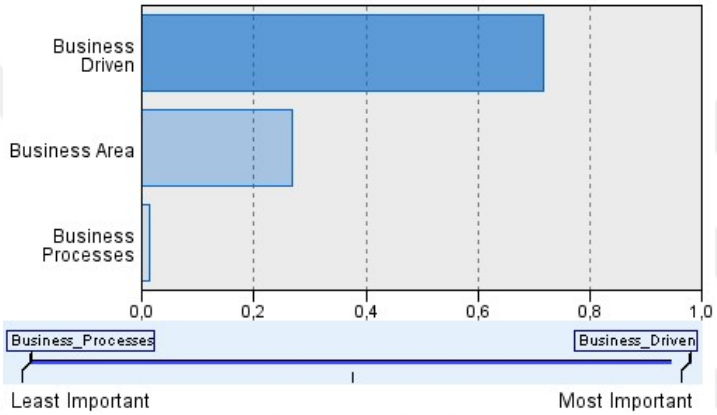
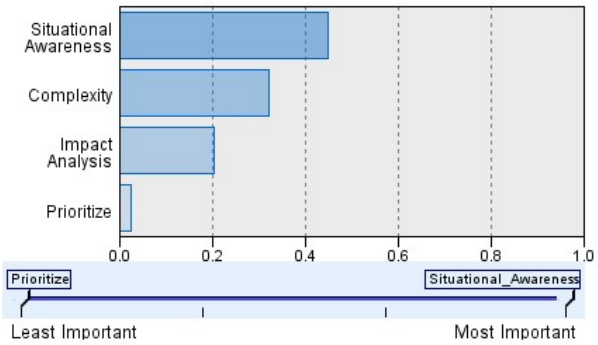


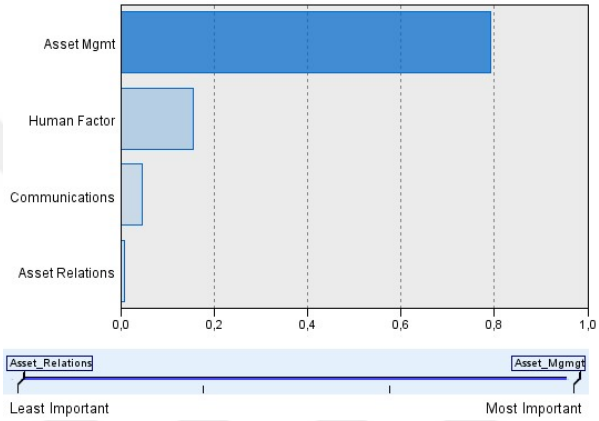
Figure 29 shows that situational awareness is the most important predictor of better investment decisions. In this analysis, respondents are asked whether enterprise architecture approach in cybersecurity management may increase the situational awareness and it is observed that they are agreed. They also agreed that the other predictors: enterprise architecture approach reduces complexity, provides better risk management with business impact analysis and facilitates prioritization.

Figure 29: Predictors of Convenient Investment Decisions



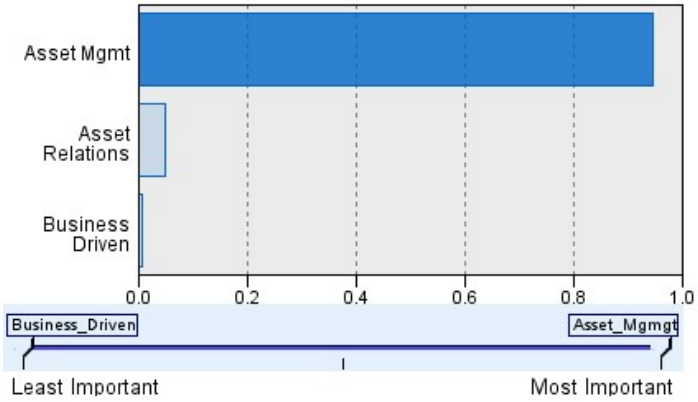
As Figure 30 the asset management is the most important predictor of all cybersecurity functions. The Cybersecurity Framework has developed by NIST also emphasize the asset management in itself (*Framework for Improving Critical Infrastructure Cybersecurity VER 1 1*, 2018).

Figure 30: Predictors of Cybersecurity Functions
(Identify, Protect, Detect, Response, Recover)



Previously, it is observed that business impact analysis is the most important function due to given choices to the respondents. Figure 31 shows that asset management not only the most important predictor of cybersecurity functions but also the most predictor of the business impact analysis.

Figure 31: Predictors of Business Impact Analysis



4.2.4. Open – Ended Questions

Respondents are asked to identify the advantages and/or disadvantages that enterprise architecture provides or possibly provide in terms of cybersecurity. It is stated by respondents that enterprise architecture methodologies may have positive effect on cybersecurity management by better risk analysis, better project planning and investment. Some responses conclude that enterprise architecture makes a holistic sight of view for cybersecurity management. It is also stated that enterprise architecture collaboration raise the awareness of business risks may cause by cyber incidents for business managers. Some explained that enterprise architecture methodologies ensure clarity and traceability of organizational assets. Some of respondents emphasize the importance of awareness raising trainings and corporate communications to minimize human induced faults. The common perception of enterprise architecture and cybersecurity management is completing each other in terms of strategy development.

CONCLUSION

Today's cybersecurity risks turn into business risks because every scale of organizations are highly dependent on information technology. Any incident that affects the information system, directly affects the quality of IT and business value. On the other hand, cost of production and reputation loss and the cost of recovering from a cyber-incident, the cost of legal obligations related cybersecurity is significant problem for businesses. Even cybersecurity seems as a technical subject, pure technology is not enough to ensure business safety itself. Moreover, the processes and the people is integral part of the cybersecurity. Good understanding of the needs and risks the business have is vital. So, cybersecurity concerns both business and IT roles, the concern belongs to the entire enterprise.

In this study, prime respondents from leading organizations, executive managers, cyber security experts and enterprise architects are interviewed. The executives, the experts and the practitioners are agreed that cybersecurity strategy strongly connected with business goals, objectives and processes. Enterprise architecture tackle with responsibility matrixes, better alignment of enabler and enhancer IT domains, reducing complexity in asset managements, serves better risk management with business impact analysis.

In the research survey and interviews, respondents find the questions clear enough and informative. Respondents are aware of adverse effects of cyber incidents to businesses. Prestigious and revenue problems are leading adverse effects that respondents threaten. It is perceived that every service may dependent another service, in this case business impact analysis gain more importance. According to the perception of responsibility, majority of respondents agree that both executives and business owners are responsible as much as cybersecurity workforce due to business safety but even minority but still some executives think that the responsibility is at IT department. Respondents agree that managerial habits affect the cybersecurity approaches. Depending the business area, legal obligations and different processes, cybersecurity management strategy varies. Majority of the respondents agree that even numerous of checklists and standards are exist, there need to be custom security alignment for enterprises. Respondents thinks that cybersecurity strategy must be

business oriented. On the other hand, it is find that there is still a ambiguity about cybersecurity management framework whether is nothing more than firewalls and antiviruses. Almost every respondent emphasizes the importance of the cybersecurity awareness, enterprise communication and human factor.

Respondents agree that alignment of business strategy and cybersecurity strategy makes the organizations' cybersecurity postures more robust and enterprise architecture is an important tool for this alignment. In addition, it is perceived that enterprise architecture driven cybersecurity led to better security investment decisions.

According to the literature review there are some approaches newly occurring in terms of cybersecurity and enterprise architecture alignment. Some researches emphasizes the benefits of cybersecurity risk management with the Zachman Framework for Enterprise Architecture. Other examples are, NIST Cybersecurity Framework collaborates with COBIT as an informative reference in related functions and there is a joint study between TOGAF and SABSA frameworks. The new version of ITIL also includes some cybersecurity articles.

In the research survey, 75% of the respondents declares that they are still practicing and will practice enterprise architecture methodologies in future. According to the responses TOGAF enterprise architecture and ITIL framework leading the industry. There are numerous positive feedbacks gives the idea about high level acceptance of this study's objectives. Respondents give additional opinions and recommendations due to collaboration of enterprise architecture and cybersecurity management especially in business impact analysis. There are almost no negative concerns such as additional costs or labour loss. Eventually, the literature and the new tendency of the industry show parallelism with the responses about the importance of enterprise architecture driven cybersecurity.

REFERENCES

Abernathy, R., & McMillan, T. (2018). *CISSP Cert Guide*.

Aier, S., Ekstedt, M., Matthes, F., Proper, E., Sanz, J. L., & (Eds.). (2010). Trends in Enterprise Architecture Research and Practice-Driven Research on Enterprise Transformation. In *An Overview of BPMN 2.0 and Its Potential Use*. https://doi.org/10.1023/A:1005132430171

Amit, R., & Zott, C. (2001). Value Creation in E-Business. *Strategic Management Journal*, *22*(6–7), 493–520. https://doi.org/10.1002/smj.187

Andress, J. (2014). *The Basics of Information Security Second Edition The Basics of Information Security Understanding the Fundamentals of InfoSec in Theory and Practice Second Edition*.

Bloomberg, J., & Schmelzer, R. (2013). The Agile Architecture Revolution: How Cloud Computing, REST-Based SOA, and Mobile Computing are Changing Enterprise IT. In *Journal of Chemical Information and Modeling* (Vol. 53).

Brennen, J. S., & Kreiss, D. (2016). Digitalization. *The International Encyclopedia of Communication Theory and Philosophy*, *89*(16), 1–11. https://doi.org/10.1001/jama.1927.02690160061030

Burmeister, F., Drews, P., & Schirmer, I. (2019). A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, *6*, 6052–6061.

Carey, M. J., & Jin, J. (2019). *Tribe of Hackers*.

Carr, D., & Else, S. (2018). *State of Enterprise Architecture Survey: Results and Findings*. (May), 2–15.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems*, *106*(3), 345–361. https://doi.org/10.1108/02635570610653498

Choejey, P., Fung, C. C., Wong, K. W., Murray, D., & Sonam, D. (2015). Cybersecurity challenges for Bhutan. *ECTI-CON 2015 - 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, 1–5. https://doi.org/10.1109/ECTICon.2015.7206975

Data Breach Investigations Report. (2018).

End of Year Data Breach Report. (2018).

Engelsmana, W., Quartelc, D., Jonkersa, H., & van Sinderen, M. (2011). Extending enterprise architecture modelling with business goals and requirements. *Enterprise Information Systems*, *5*(1), 9–36. https://doi.org/10.1080/17517575.2010.491871

Ezingeard, J. N., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. *Journal of General Management*, *32*(4), 53–72. https://doi.org/10.1177/030630700703200404

Framework for Improving Critical Infrastructure Cybersecurity VER 1 1. (2018). https://doi.org/10.6028/NIST.CSWP.04162018

Gantz, S. D. (2013). FISMA and the Risk Management Framework. In *Phase I*. https://doi.org/10.1016/B978-0-12-396959-0.00001-X

Gavilan, J. (2016). *The state of cybersecurity in the Philippines*. Retrieved from https://www.rappler.com/newsbreak/in-depth/130883-state-cybersecurity-philippines

Giaglis, G. M., Mylonopoulos, N., & Doukidis, G. I. (1999). The ISSUE Methodology for Quantifying Benefits from Information Systems. *Logistics Information Management*, *12*, 52–62.

Hinkelmann, K. (2012). *Enterprise Architecture*.

Hoque, R., Liendo, C., & Chesson, A. L. (2009). A Taxonomy of Operational Cyber Security Risks. *Journal of Clinical Sleep Medicine*, *5*(3), 277–279. https://doi.org/10.1007/978-1-4419-7133-3

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Insider Threat Program Guide. (2019).

Jalaliniya, S., & Fakhredin, F. (2011). *Enterprise Architecture & Security Architecture Development*. Retrieved from http://www.enterprisearchitecture.ir/downloads/thesis/Thesis_Shahram%26Farzaneh.pdf

Janssen, M. (2009). *Framing Enterprise Architecture: A Meta-Framework For Analayzing Architectural Efforts In Organizations*. Retrieved from https://courses.edx.org/c4x/DelftX/NGI102x/asset/Framing_Enterprise_Architecture.pdf

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond Cybersecurity: Protecting Your Digital Business*. Retrieved from https://books.google.com/books/about/Beyond_Cybersecurity.html?id=mi69BgAAQBAJ

Kayworth, T., & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive*, *9*(3), 15.

Knapp, K. J. (2014). *The Top Information Security Issues Facing Organizations: What Can Government Do to Help? Information Security Effectiveness in Organizations View project*. (2006), 2019. https://doi.org/10.1201/1079.07366981/46351.34.4.20061001/95104.1

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The Association between Top Management Involvement and Compensation and Information Security Breaches. *Journal of Information Systems*, *27*(1), 219–236. https://doi.org/10.15709/hswr.2012.32.4.219

Landthaler, J., Kleehaus, M., & Matthes, F. (2016). Multi-level event and anomaly correlation based on enterprise architecture information. *Lecture Notes in Business Information Processing*, *272*, 52–66. https://doi.org/10.1007/978-3-319-49454-8_4

Ma, Q., Schmidt, M., & Pearson, J. (2009). An integrated framework for information security management. *St John's University Review of Business*, *30*(1), 58–69. Retrieved from https://www.stjohns.edu/sites/default/files/documents/Tobin/volume30-number1-fall2009.pdf#page=60

Mayer, N., Aubert, J., Grandry, E., & Feltus, C. (2016). An integrated conceptual model for information system security risk management and enterprise architecture management based on TOGAF. *Lecture Notes in Business Information Processing*, *267*, 353–361. https://doi.org/10.1007/978-3-319-48393-1_27

McDowall, J. D. (2019). Complex Enterprise Architecture. In *Complex Enterprise Architecture*. https://doi.org/10.1007/978-1-4842-4306-0

Mowbray, T. J. (2014). *Cybersecurity - Managing Systems, Conducting Testing, and Investigating Intrusions*. https://doi.org/10.1017/CBO9781107415324.004

Nielsen, S. C. (2012). Pursuing Security in Cyberspace: Strategic and Organizational Challenges. *Orbis*, *56*(3), 336–356. https://doi.org/10.1016/j.orbis.2012.05.004

Niemi, E. (2006). Enterprise architecture benefits: Perceptions from literature and practice. *International Business Information Management (IBIMA)*, *14*, 16.

Nunnally, J. C. (1978). *Psychometric Theory* (2nd ed.). New York: McGraw-Hill.

Penber-Bey, G. (2012). *The Parkerian Hexad: The CIA Triad Model Expanded*.

Poe, L. (2018). *The Development of Information Assurance and Cybersecurity Competency Lists*. (August).

Promis, A., Ag, S., & McLeod, G. (2008). The Inspired Enterprise Architecture Frameworks. *Interfaces*, 1–28. Retrieved from http://http//www.pro-mis.com/resources.html

Proper, E., Lankhorst, M. M., Schönherr, M., Barjis, J., Overbeek, S., & (Eds.). (2010). Trends in Enterprise Architecture Research. In *Lecture Notes in Business Information Processing*. https://doi.org/10.1007/978-3-642-33155-8

Proper, H. A., & Lankhorst, M. M. (2014). Towards essential sensemaking. *Enterprise Modelling and Information Systems Architecture*, *9*(1), 5–21.

Rachinger, M., Rauter, R., Müller, C., Vorraber, W., & Schirgi, E. (2018). Digitalization and its influence on business model innovation. *Journal of Manufacturing Technology Management*. https://doi.org/10.1108/JMTM-01-2018-0020

Rohmeyer, P., & Bayuk, J. L. (2018). Financial Cybersecurity Risk Management. In *Financial Cybersecurity Risk Management*. https://doi.org/10.1007/978-1-4842-4194-3

Rot, A. (2009). Enterprise Information Technology Security: Risk Management Perspective. *Proceedings of the World Congress on Engineering and Computer Science 2009*, *II*, 6. Retrieved from https://pdfs.semanticscholar.org/35bc/4d37f9c84046bf9cdf084172d3740b81d2c2.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students* (6, Ed.).

Schwab, W., & Poujol, M. (2018). *The State of Industrial Cybersecurity 2018*. (June).

Sherwood, J., Clark, A., & Lynas, D. (2009). Enterprise Security Architecture (SABSA) White Paper. *(Sabsa)*, 25. https://doi.org/10.1108/02635570510616111

Sifaleras, A. (2019). *Operational Research in the Digital Era – ICT Challenges*. https://doi.org/10.1007/978-3-319-95666-4

Sigler, K. E. (2018). Securing an IT Organization through Governance, Risk Management, and Audit. In *Securing an IT Organization through Governance, Risk Management, and Audit*. https://doi.org/10.1201/b19194

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239. https://doi.org/10.1007/s40171-013-0047-4

Solms, R. von. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*, (3), 224–225.

Solms, R. von, & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Soomro, Z. A., Hussain, M., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. Retrieved from http://10.0.3.248/j.ijinfomgt.2015.11.009%0Ahttp://libaccess.sjlibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=lls&AN=111823932&site=ehost-live&scope=site

Susanto, H., & Almunawar, mohammad nabil. (2018). Information Security Management Systems. In *Apple Academic Press*. https://doi.org/10.1201/9780203486061.ch3

The Open Group TOGAF-SABSA Integration Working Group. (2011). TOGAF ® and SABSA ® Integration. In *Sabsa*. Retrieved from https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12449

Thompson, E. C. (2018). Cybersecurity Incident Response. In *Cybersecurity Incident Response*. https://doi.org/10.1007/978-1-4842-3870-7

Threatscape Report 2018 Midyear Cybersecurity. (2018).

Tisdale, S. M. (2015). Cybersecurity: Challenges From a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues in Information Systems*, *16*(3), 191–198. Retrieved from https://pdfs.semanticscholar.org/5e0b/b009f7b87d3fff87b20e156a56a726f891fb.pdf%0Ahttp://www.iacis.org/iis/2015/3_iis_2015_191-198.pdf

Urbaczewski, L., & Mrdalj, S. (2006). A COMPARISON OF ENTERPRISE ARCHITECTURE FRAMEWORKS. *Issues in Information Systems*, *2*(2), 18–23. https://doi.org/10.1227/01.neu.0000410082.42657.aa

Warsinke, J., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., … Vasquez, M. (2019). *The Official (ISC) 2 ® CISSP® CBK® Reference*.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43–57. https://doi.org/10.1016/j.ijinfomgt.2003.12.003

Young, R. F., & Windsor, J. (2010). Empirical Evaluation of Information Security Planning and Integration Empirical Evaluation of Information Security Planning and Empirical Evaluation. *Information Security*, *26*(March), 245–266. https://doi.org/10.17705/1CAIS.02613

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal*, *26*, 276–292. https://doi.org/10.1147/sj.382.0454

APPENDICES

Appendix 1: Interviews Questions

Question 1: Have you ever experienced and or implemented any enterprise architecture methodologies to your organization, if so which one / ones?

Question 2: What are the main benefits of enterprise architecture practices to your organization?

Question 3: What are the main struggles of managing risk in terms of cybersecurity?

Question 4: How do you realize business impact analysis of cyber incidents?

Question 5: What do you think about the relation of cybersecurity risks and business risks?

Question 6: How do you align business strategy with IT and cybersecurity strategy?

Question 7: What aspects of enterprise architecture and cybersecurity management collaboration can be beneficial?

Question 8: Would you please share any other contribution to realize better cybersecurity management?

Appendix 2: Survey

Enterprise Architecture and Cybersecurity

This survey has been prepared within the scope of my master's thesis at Dokuz Eylül University, Izmir, Turkey.

The thesis subject is "Enterprise Architecture Driven Cybersecurity".

The main purpose of this research is to discuss the effects of enterprise architecture methodologies on cybersecurity management.

Your e-mail and name - surname information will not be shared with 3rd parties.

The answers given in the questionnaire will not be used except for scientific researches.

If you would like to have more information about the study, please contact the researcher at barsaybars@gmail.com

Thank you for your participation.

* Required

Name, Surname (Optional)

Your answer

E-mail (Optional)

Your answer

Select the option that best describes your job role. *

- [ ] Software Developer
- [ ] Information Technology Specialist
- [ ] Information Technology Manager
- [ ] Information Security / Cybersecurity Specialist
- [ ] Information Security / Cybersecurity Manager
- [ ] Project Manager
- [ ] Executive Manager
- [ ] Enterprise Architecture Specialist
- [ ] Other: _____

Number of Employees in Your Organization *

- ○ Less than 10
- ○ 10 - 49
- ○ 50 - 249
- ○ More than 250

Sector *

- [ ] Public
- [ ] Private
- [ ] Other: _____

Cyber Incidents (e.g., Attack, Malicious Activity, System Failure)

Which of the following would adversely affect your organization? (If you have a selection other than All and None, you can mark more than one.) *

- [ ] Consequences of regulatory requirements
- [ ] Prestige
- [ ] Effort
- [ ] Revenue
- [ ] External Stakeholders
- [ ] All of them
- [ ] None of them

Causes risk for business continuity. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

A service effected negatively may affect other dependent services. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

May cause serious losses for organizations. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Cybersecurity (Information Security, ICT Security, Business Security)

Is the responsibility of the top management directly. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Is one of the responsibilities of business process owners. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Cybersecurity Strategy

Depends on the field of activity of the organization. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Is being shaped according to legal obligations. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Varies according to different business processes. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Cybersecurity Strategy

Should be business oriented. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Should involve all cybersecurity functions *. *

* Identification, Protection, Detection, Response, Recover

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Should identify the relationship of the assets (e.g., services, applications) to each other. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

* Required

Cybersecurity is perceived as hardware and software. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Administrative habits affect cyber security management. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Awareness / knowledge level of cybersecurity of employees is important. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Corporate communication is important in cybersecurity. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Human factor (e.g., sense of belonging, reliability) is important in cybersecurity. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Enterprise Architecture Approach in Cybersecurity Management

Ensures that business strategy and cybersecurity strategy are aligned. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Provides effective asset management. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Reduces complexity. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Increases situational awareness. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Facilitates prioritization. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Provides better risk management with business impact analysis. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Enterprise Architecture Approach in Cybersecurity Management

Reduces costs by helping for more convenient investment decisions. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

****

* Required

In my organization *

- ○ Enterprise architecture methodology is applied.
- ○ It is planned to adopt / adapt an enterprise architecture methodology in the future.
- ○ I've never heard of enterprise architecture before, I learned it through this survey.
- ○ There is no enterprise architecture practice and it is not planned in near future. (Continue skipping the next question.)

Please specify the enterprise architecture methodology / business framework that your organization applies / will apply.

- ☐ TOGAF
- ☐ COBIT
- ☐ SABSA
- ☐ Zachman
- ☐ ITIL
- ☐ Other: _____

Enterprise Architecture and Cybersecurity

Did you get any new idea about enterprise architecture through this survey? Or is your existing idea changed? (Optional)

Your answer

Did you get any new idea about cybersecurity management through this survey? Or is your existing idea changed? (Optional)

Your answer

Please identify the advantages / disadvantages that enterprise architecture provides / can provide in terms of cybersecurity. (Optional)

Your answer

Please provide your feedback on this survey. (Optional)

Your answer

THANK YOU FOR YOUR PARTICIPATION.