
Jani Päivärinta

# Strategic Management of the Organizations Cybersecurity

Conceptual Model of the Structure, Principles, and the Best Practices for Organizational Cybersecurity Excellence

School of Technology and Innovations
Master's Thesis
Industrial Systems Analytics

Vaasa 2022

**VAASAN YLIOPISTO**
**Tekniikan ja innovaatiojohtamisen yksikkö**
**Tekijä:** Jani Päivärinta
**Tutkielman nimi:** Organisaatioiden kyberturvallisuuden strateginen johtaminen : Organisaation kyberturvallisuuden huippuosaamisen rakenteen, periaatteiden ja parhaiden käytäntöjen konseptuaalinen malli
**Tutkinto:** Diplomi-insinööri
**Oppiaine:** Industrial Systems Analytics
**Työn ohjaaja:** Binod Timilsina
**Valmistumisvuosi:** 2022 **Sivumäärä:** 74

**TIIVISTELMÄ:**
Organisaatioiden ylin johto näkee kyberturvallisuusuhat yhtenä suurimmista huolenaiheista, ja heillä on siihen hyvä syy. Kyberhyökkäykset ovat lisääntyneet kaikkialla maailmassa niin mittakaavaltaan kuin kehittyneisyydeltäänkin. Sääntelyviranomaiset vaativat organisaatioita suojaamaan käyttäjätietojaan ankarilla rangaistuksilla, mikäli organisaatiot eivät noudata viranomaisten vaatimuksia. Tämä tutkimus pyrkii vastaamaan tähän huolenaiheeseen selvittämällä, että mitä organisaatioissa on viime aikoina tehty? Ja tämän ymmärryksen pohjalta kehittämään uuden konseptuaalisen mallin, jonka avulla organisaatiot voivat parantaa strategista kyberturvallisuuden johtamista. Tutkimus alkaa kahdella tutkimuskysymyksellä: Mikä on organisaatioiden nykytilanne strategisen kyberturvallisuuden johtamisen alalla? ja millaisia malleja, rakenteita, periaatteita ja käytäntöjä meidän on kehitettävä saavuttaaksemme organisaation kyberturvallisuuden huippuosaamisen?

Tämä tutkimus on toteutettu kvalitatiivisten ja kvantitatiivisten tutkimusmenetelmien yhdistelmällä. Alkaen laajasta kirjallisuuskatsauksesta ja teoreettisesta viitekehyksestä viimeisimmästä tieteellisestä tutkimuksesta käyttäen kvalitatiivista tutkimusmenetelmää. Ja jatkaen pääosin toissijaisella, mutta myös primäärisellä tiedonkeruulla käyttäen kvantitatiivista tutkimusmenetelmää. Molempia tutkimusmenetelmiä käytetään vastaamaan samoihin tutkimuskysymyksiin. Vertailevaa ja kuvailevaa analyysiä käytetään erilaisten suureiden ja näkökulmien ymmärtämiseen sekä alan strategisen kyberturvallisuuden johtamisen nykytilanteen ymmärtämiseen.

Kirjallisuuskatsauksen, teoreettisen viitekehyksen, esitettyjen kyberturvallisuusstandardien ja -kehysten, syvällisen analyysin, tutkijan havaintojen, muiden havaintojen, tutkijan empiirisen kokemuksen perusteella ja tämän tutkimuksen aikana esiin tulleiden parannusideoiden pohjalta kehitetään uusi konseptuaalinen strategisen kyberturvallisuuden johtamismalli organisaatioiden tueksi. Konseptuaalinen malli on viitekehys ja sisältää kolme strategista valintaa, jotka voivat toimia ohjaavina periaatteina tai käytäntöinä parantamaan organisaation kyberturvallisuutta.

Tämän tutkimuksen kontribuutio on se, että siinä ehdotetaan kolmea strategista valintaa, joita organisaatioiden tulisi käyttää parantaakseen strategista kyberturvallisuuden johtamista ja siirtyäkseen kohti kyberturvallisuuden huippuosaamista. Nämä kolme ehdotettua strategista valintaa ovat täydellinen omistajuus, joka on kiistanalainen nykytrendille, turvallinen suunnittelu, jota ei tavallisesti käytetä, ja rajavalvonta, jota voidaan verrata maiden rajavalvontaan, mutta kyberavaruudessa. Malli on esitetty tässä tutkimuksessa yksinkertaisilla suoritusesimerkeillä, eikä se sulje pois muita strategisia kyberturvallisuuden johtamiskäytäntöjä.

**AVAINSANAT:** Strateginen johtaminen, Kyberturvallisuus, Järjestelmäsuunnittelu, Konseptuaalinen malli

**UNIVERSITY OF VAASA**
**School of Technology and Innovations**
**Author:** Jani Päivärinta
**Title of the thesis:** Strategic Management of the Organizations Cybersecurity: Conceptual Model of the Structure, Principles, and the Best Practices for Organizational Cybersecurity Excellence
**Degree:** Master of Science in Technology
**Discipline:** Industrial Systems Analytics
**Supervisor:** Binod Timilsina
**Year:** 2022 **Pages:** 74

**ABSTRACT :**
Top management sees cybersecurity threats as one of the biggest concerns to their organisations and they have a good reason. Cyberattacks are increasing all over the world in scale and in sophistication. Regulators are demanding that organisations protect their user data with severe penalties if organization fails to comply. This study aims to address that concern by studying what has been done lately and based on that understanding by developing a new conceptual model that organisations can use to improve their strategic cybersecurity management. Research starts with two research questions: What is the current situation of the organisations in the field of strategic cybersecurity management? and what kind of models, frameworks, principles, and the practices we need to develop to achieve organizational cybersecurity excellence?

This study is conducted by using mixed methods research approach. Starting from extensive literature review and theoretical framework from the latest scientific research by using qualitative research method and continuing with mainly secondary but also primary data collection by using quantitative research method. Both research methods are used to answer same research questions. Comparative and descriptive analysis is used to understand different quantities and perspectives, and to understand current situation in the field strategic cybersecurity management.

Based on the literature review, theoretical framework, presented cybersecurity standards and frameworks, in-depth analysis, researcher's observations, other findings, researcher's empirical experience, and surfaced improvement ideas during this study, a new conceptual strategic cybersecurity management model is developed to improve organisations strategic cybersecurity management. Conceptual model is a framework and contains three strategic choices that can act as guiding principles or practices to improve organisations cybersecurity.

Originality of this study is that it proposes three strategic choices that organisations should use to improve their strategic cybersecurity management and to move towards cybersecurity excellence. These three proposed strategic choices are complete ownership which is controversial to current trend, secure by design which is not normally used and border control which can be compared to nations border control but in cyberspace. Model is represented in this study with simple execution examples and does not exclude any other strategic cybersecurity management practices.

**KEYWORDS:** Strategic Management, Cybersecurity, Systems Engineering, Conceptual Model

## Contents

## Figures



## Tables

## Abbreviations

| | |
|---|---|
| ACSC | Australian Cyber Security Centre (Australia) |
| APT | Advanced Persistent Threat |
| BYOD | Bring Your Own Device |
| CCAM | Cybersecurity Competitive Advantage Model |
| CTI | Cyber Threat Intelligence |
| CDPA | The Consumer Data Protection Act (United States) |
| CMM | Cybersecurity Capacity Maturity Model for Nations (CMM) |
| CIS | Center of Internet Security |
| CSAT | Cybersecurity Awareness Training |
| DIBR | Data Investigations Breach Report (Verizon) |
| DPC | Data Protection Commission (Ireland) |
| CISA | Cybersecurity & Infrastructure Security Agency (United States) |
| ENISA | European Union Agency for Cybersecurity |
| EU | European Union |
| GCSCC | Global Cyber Security Capacity Centre (Oxford University) |
| GDPR | The General Data Protection Regulation (EU) |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IT | Information Technology |
| ISO | International Organization for Standardization |
| ISMS | Information Security Management System |
| M-TISM | Modified Total Interpretive Structural Model |
| NCAF | National Capabilities Assessment Framework |
| NCSC | National Cyber Security Centre (United Kingdom) |
| NCSC-FI | National Cyber Security Centre (Finland) |
| NIST | National Institute of Standards and Technology (United States) |
| PCI | Payment Card Industry |
| PCI DSS | Payment Card Industry Data Security Standard |
| PCS | People-Centric Security |
| S-APT | Strategically Motivated Advanced Persistent Threat |

# 1 Introduction

This chapter is about introduction to this research. What is this research about? Why is this research conducted? and how this research is going to be conducted? This chapter will look to the background and the purpose of this research, identify the current research gap, formulates the research questions, and construct research objectives based on those formulated research questions. This chapter also describes how the actual research process is conducted. Topic of this research is strategic cybersecurity management which can be applied to all types of public and private sector organizations, big and small.

## 1.1 Background

Are cybersecurity threats a major reason behind the sleepless nights of the top management all over the world? According to Kosutic and Pigni (2021) "top executives see cyberattacks as one of the biggest global threats to their businesses" (p. 28) while Rajan et al. (2021) points out that "cybersecurity is a serious issue that many organizations face these days" and "therefore, cybersecurity management is very important for any organization" (p. 120872). Some researchers even point out that "cyberattacks can be more dangerous than guns and tanks" (Carvalho et al., 2020, p. 1845) by referring to the EU President Jean-Claude Juncker's 2017 state of the union speech where he stated that "cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks" (European Commission, 2017) and he didn't stop there but stated in that same speech that "last year alone there were more than 4000 ransomware attacks per day and 80% of European companies experienced at least one cyber-security incident" (European Commission, 2017). But arguing cyberattacks as being "more dangerous than guns and tanks" is small concern to the top management compared to what Senator Ron Wyden had been proposing in the Consumer Data Protection Act (CDPA) bill in the United States, 20 years of jail time "for executives who knowingly sign off on incorrect or inaccurate annual certifications of their companies' data-security practices" (Wolff as cited in Chatterjee, 2019). Talking

about demanding responsibility from the top management. In 2018, Mori and Goto (2018) stated that "damages caused by cyber-attacks are becoming larger, broader and more serious" (p. 957). Global Cyber Security Capacity Centre (GCSCC) at Oxford University by Dutton et al. (2022) on their article "Next Steps for the EU: Building on the Paris Call and EU Cybersecurity Strategy" stated that "cybersecurity has become an increasingly important concern across the European Union and the globe as the internet has become more central and attacks on this infrastructure of the digital age have grown in scale and sophistication" (p. 1).

According to European Parliament (2022) here in Europe cybersecurity threats has been on the raise. Global consulting firm McKinsey & Company and their McKinsey's Risk & Resilience Practice has come to same conclusions, cyberattacks are on the raise (Boehm et al., 2022). From April 2020 to July 2021 top sectors that have been influenced by cybersecurity threats here in the Europe are the public administration and government, digital service providers, public, health care and financing (European Union Agency for Cybersecurity as cited in European Parliament, 2022) but McKinsey's Risk & Resilience Practice adds that nobody seems to be immune to cyber threats (Boehm et al., 2022). Worldwide software company Microsoft's Security states that from July 2020 to June 2021 ransomware attacks raised 1070 % (Fortinet Ransomware Survey Report as cited in Jakkal, 2022) while US-based Cybersecurity & Infrastructure Security Agency (CISA) and UK-based National Cyber Security Centre (NCSC) stated that US, Australia and UK authorities has jointly witnessed a raise in "ransomware incidents against critical infrastructure" (Cybersecurity & Infrastructure Security Agency, 2022; National Cyber Security Centre, 2022). American business magazine Fortune stated that while the entire globe faced a 105% raise in ransomware attacks, health care faced a 755% raise but governments all over the world faced a 1885 % raise in ransomware attacks in 2021 (2022 Cyber Threat Report as cited in Taylor, 2022). In the UK, small businesses faced a 62% raise in cybersecurity threats (Software Advice report as cited in Irwin, 2022). Australian Cyber Security Centre (ACSC) stated on their annual cyber threat report that from July 2020 to June 2021 they witnessed 15 % raise in ransomware cybercrime

reports while overall reported cybercrimes raised 13 % (Australian Cyber Security Centre, 2022). In November 2021 Finland was fighting against malware attacks, defined as exceptional, Finnish National Cyber Security Centre (NCSC-FI) and two big telecommunication companies Telia and Elisa were all involved (Pohjanpalo, 2021).

Overall, we can conclude that top management concerns about cybersecurity threats are not in any way baseless. Cybersecurity threats seem to be increasing all over the world and no one seems to be safe from them. Cyberattacks also seems to be more sophisticated which requires high level of skill to conduct such as ransomware attacks, and above everything else, having legislators threatening executives with jail time, I wouldn't be surprised if top management sees cyber threats as one of their top concerns.

## 1.2 Purpose of the Research

The purpose of this research is to find out what kind of strategic cybersecurity management practices organizations currently use or have been using, what is the scientific research focus in the field of strategic cybersecurity management, and in what way organisations strategic cybersecurity management can be improved?

## 1.3 Problem Statement

While cybersecurity is seen globally to be a serious concern for different kind of organizations (Kosutic& Pigni, 2021; Rajan et al., 2021; Carvalho et al., 2020; European Commission, 2017; Dutton et al., 2022) and that cyberattacks are currently increasing all over the world (European Parliament, 2022; Boehm et al., 2022; Jakkal, 2022; Cybersecurity & Infrastructure Security Agency, 2022; National Cyber Security Centre, 2022; Taylor, 2022; Irwin, 2022; Australian Cyber Security Centre, 2022; Dutton et al., 2022) the question is: How can we improve organization's strategic cybersecurity management to minimize these concerns?

## 1.4 Research Gap

Strategic cybersecurity management has been studied in scientific communities such as universities and military academies around the world. Different kind of strategies has been presented in scientific literature lately and wide range of cybersecurity management frameworks has been created to help organisations. Table 1 below shows the latest scientific research contributions in the field of strategic cybersecurity management.

| **Author(s)** | **Research Focus** |
|---|---|
| Kosutic, D., & Pigni F. (2021) | How can cybersecurity improve competitive advantage? How to use strategic framework of Cybersecurity Competitive Advantage Model (CCAM) to build competitive advantage. |
| Rajan et al. (2021) | Identify the factors that affect cybersecurity within organization and analyse relationships among these factors by using modified total interpretive structural modelling (M-TISM) technique. |
| Ogbanufe et al. (2021) | Understand the top manager's role in cybersecurity strategy, specifically with cyberinsurance by collecting data from executive-level managers. |
| Hepfer, M., & Powell, C. (2020) | How to use cybersecurity as a strategic asset. |
| Borum et al. (2015) | Highlight the importance and role of strategic cyber intelligence to support risk-informed decision making. |
| Ahmad et al. (2019) | What is advanced persistent threat? This study explains how strategically motivated advanced persistent threats (S-APTs) conduct their strategic cyberattacks by using different ways and how to counter to these attacks. |
| Pang, M. S., & Tanriverdi, H. (2022) | Modernization of Information Technology (IT) vs. legacy IT security debate. How modernization or cloud migration can be used to minimize cyber risks? |
| Galinec et al. (2018) | National level strategic approach to cybersecurity and cyberdefense. |

| | |
|---|---|
| He et al. (2020) | Cybersecurity awareness training. Investigate the effect of different evidence-based cybersecurity training methods on employee's cybersecurity risk perception and self-reported behaviour. |

**Table 1.** Latest scientific research on strategic cybersecurity management.

Table 2 below shows some of the cybersecurity management standards and frameworks which organizations currently use.

| **Author** | **Description** |
|---|---|
| NIST - National Institute of Standards and Technology (2018) | NIST framework for improving critical infrastructure cybersecurity |
| ISO - International Organization for Standardization (2013) | ISO/IEC 27001:2013 |
| ISO - International Organization for Standardization (2013) | ISO/IEC 27002:2013 |
| CIS - Center for Internet Security (2022) | The 18 CIS Critical Security Controls |
| PCI - Payment Card Industry Security Standards Council (2022) | Payment Card Industry Data Security Standard (PCI DSS) |
| ENISA - European Union Agency for Cybersecurity (2020) | National Capabilities Assessment Framework (NCAF) |

**Table 2.** Cybersecurity management standards and frameworks.

While the latest research on strategic cybersecurity management has focused on many single aspects of the strategic cybersecurity management, holistic view of the matter is still missing. Some of the used standards and frameworks try to fill this gap by generating a framework which organisations can use to holistically manage their cybersecurity, but these standards and frameworks has not yet really solved the overall concern, organisations are still under different kind of cyber threats and cyberattacks are globally increasing in amount and in sophistication, and something needs to be done to address these concerns.

## 1.5 Research Questions

Based on the understanding that cybersecurity is a serious concern of senior executives and that the current situation of the strategic cybersecurity management is not really solving the problem, the following research questions has been formulated.

Research questions:

1. What is the current situation of the organizations in the field of strategic cybersecurity management?
2. What kind of models, frameworks, principles, and the practices we need to develop to achieve organizational cybersecurity excellence?

## 1.6 Research Objectives

This research will examine existing scientific literature on strategic cybersecurity management and the different cybersecurity management standards, and frameworks which organizations use to achieve following research objectives.

Research objectives:

1. To study the current situation of the organization's cybersecurity management (past and present)
2. Based on those research findings, propose a new conceptual strategic cybersecurity management model to minimize organisations cybersecurity concerns (future)

## 1.7 Research Process

This section describes how this thesis is formally structured and how the research process is conducted so that it should be replicable by other researchers.

### 1.7.1 Structure of the Thesis

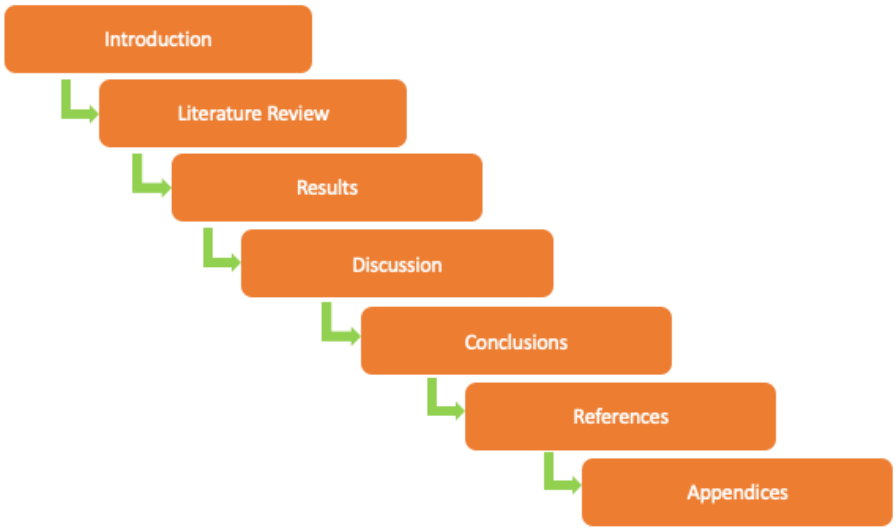


**Figure 1.** Structure of the thesis.

This thesis is structured to chapters as shown in Figure 1 above. Each chapter except references and appendices contains one or more sections.

*Introduction chapter* highlights the background of the study, importance of the strategic cybersecurity management, the purpose of this research, problem statement, research gap, research questions, research objectives and the research process.

*Literature review chapter* is purposefully divided to two sections. First section contains the latest scientific research in the field of strategic cybersecurity management to understand where the current research focus of the strategic cybersecurity management is. Second section contains short introductions to the cybersecurity standards and frameworks which organizations use.

*Results* chapter contains research description, information about data collection with limitations and delimitations, and analysis. In this chapter secondary data collection is

mainly used. Primary data collection is only used to compare results between secondary and primary data. Comparative and descriptive analysis is used in the analysis process.

*Discussion* chapter is about presenting the conceptual model with small execution examples. Based on the observations and findings of the literature review and analysis, and the earlier empirical experience, conceptual model is formulated in this chapter to improve organisations cybersecurity.

*Conclusions* chapter is about summarizing the research, talking about research contributions, evaluating reliability and validity of this research, and proposing possible future research topics that has surfaced from this research.

*References* chapters contains all the references used in this research paper in alphabetical order. APA style has been used in reference list. Most references also contain links to the original sources.

*Appendices* contains supplementary information that does not belong to the body of this thesis but might have influenced to proposed conceptual model. Appendices are mainly samples taken from the primary data.

### 1.7.2 Research Methods

This research is conducted by using mixed methods research approach as shown in Figure 2 below.

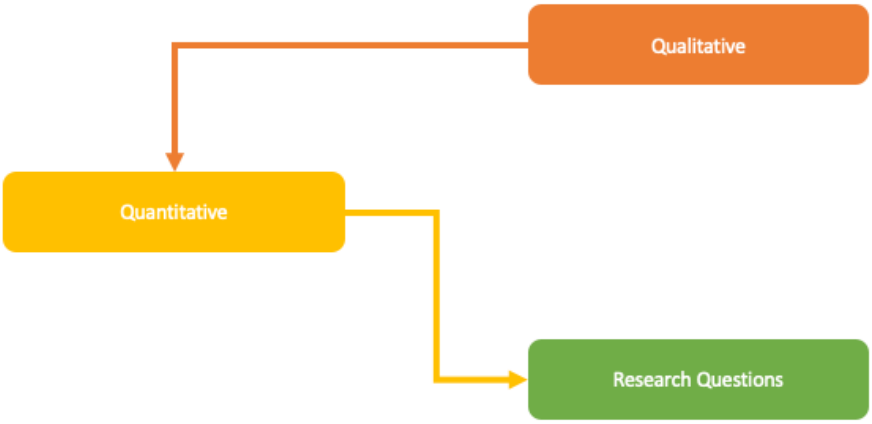


**Figure 2.** Mixed methods research process.

Research process starts by using qualitative research methods and then changing to quantitative research methods. These are done sequentially, one after another but they both answer to same research questions.

*Qualitative research methods* are used to explore current situation (past and present) from the topic "strategic cybersecurity management" from existing scientific journals, scientific articles, books written by scientist and other scientific literature. Process is descriptive in nature and tries to capture main points of the latest scientific research which are relevant to this research.

*Quantitative research methods* are used in secondary data and primary data collection process by collecting numerical data (quantities) from mainly secondary data sources but also primary data sources which are then presented in descriptive or comparative manner and analyzed. Secondary data collection is used to save time and make this research work more efficient based on the time constraint and the scope of this thesis.

### 1.7.3 Systematic Research Approach

Entire research process is conducted systematically in step-by-step manner by starting from introduction chapter and ending to the conclusions chapter. Then, feedback loop is used to repeat the research process as shown in figure 3 below.

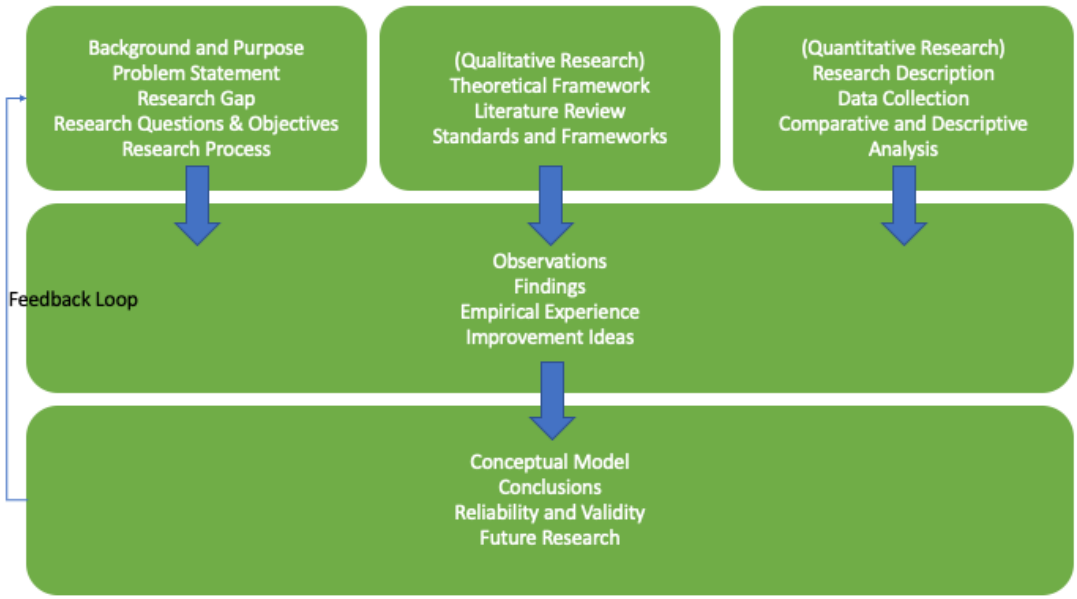


**Figure 3.** Systematic research approach.

Research starts from introduction chapter and is followed by literature review chapter which is conducted by using qualitative research method. After literature review, results chapter is conducted by using quantitative research method along with comparative and descriptive analysis.

Observations and findings are made throughout the process. Empirical experience also influences on the research and along the way improvement ideas are surfacing. These improvement ideas are then used to form conceptual model which researcher thinks would mostly improve organisations current strategic cybersecurity management. Conclusion is written by summarizing the research. Reliability and validity are evaluated, and the future research topics are presented. After this the entire process is repeated.

# 2 Literature Review

This chapter is about literature review. Purpose of this chapter is to formulate definitions and to present essential studies and theories related to strategic cybersecurity management. I have divided these studies and theories in two categories: Strategic cybersecurity management which contains studies and theories about strategic cybersecurity management and to information security management frameworks and standards which contains frameworks and standards to manage organization's cybersecurity.

## 2.1 Definitions of Strategic Cybersecurity Management

This section is about the definitions related to this research.

### 2.1.1 Definition: Strategy

What is strategy? According to Cambridge Dictionary (n.d.) strategy is defined as "a detailed plan to achieve success" while according to Merriam-Webster (n.d.) strategy is defined as "a careful plan or method".

Lawrence Freedman (2013) in his book "Strategy" gives three origins for the strategy: the Evolution, the Bible, and the Greeks, from which the last is "the most important" (p. 22). The word "strategos" which comes from Greek language, is translated as to "general" and while to word "strategy" has its "military origin" (Horwath, 2006, p. 1) it has found its way to the business and corporate world. In military context, there is also a word "tactics" which also has Greek origin and can be translated to "ordering of formations on the battlefield" (Horwath, 2006, p. 2).

In business world, there is wide range of different strategies. According to Porter (1996) positioning was once in the heart of the business strategy (p. 61) and in business world, the "competitive strategy is about being different" (p. 64).

### 2.1.2 Definition: Cybersecurity

What is cybersecurity? According to Cambridge Dictionary (n.d.) cybersecurity can be defined as "things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet". According to Merriam-Webster (n.d.) cybersecurity can be defined as "measures taken to protect computer or computer system (as on the internet) against unauthorized access or attack".

There is no scientific "consensus on what 'cyberspace' is" (Lorents and Ottis as cited in Jacuch, 2021). European Union Agency for Network and Information Security (2016) currently known as European Union Agency for Cybersecurity (name changed in 2019) has published "Definition of Cybersecurity - Gaps and overlaps in standardization - v1.0" on July 1, 2016, where they discuss that should we use "Cyber Security" or "Cybersecurity" spelling form (p. 10) because both are used. US-based Cybersecurity & Infrastructure Security Agency (2009) defines cybersecurity as an "art of protecting networks, device, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information". According to UK-based IT Governance (n.d.) cyber security can be defined as "the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks" and according to UK National Cyber Security Centre (n.d.) "cyber security is how individuals and organisations reduce the risk of cyber-attack". From the business world, according to IBM (n.d.) cybersecurity can be defined as "practice of protecting critical systems and sensitive information from digital attacks" and according to CISCO (n.d.) cybersecurity is defined as "practice of protecting systems, networks, and programs from digital attacks".

### 2.1.3 Definition: Management

What is management? According to Cambridge Dictionary (n.d.) management is defined as "the control and organization of something" or "the group of people responsible for

controlling and organizing a company". According to Merriam-Webster (n.d.) management is defined as "the act or art of managing: the conducting or supervising of something" or "the collective body of who manage or direct an enterprise".

### 2.1.4 Definition: Strategic Cybersecurity Management

Strategic cybersecurity management can be seen as "organization's strategic-level capability to protect information technology (IT) systems, information resources, and digital processes in an emerging cyber threat environment" (Ferdinand, 2015; Jenab and Moslehpour, 2016 as cited in Rajan et al., 2021).

## 2.2 Strategic Cybersecurity Management

In this section, some of the latest strategic cybersecurity management studies are presented in summarized manner.

### 2.2.1 Cybersecurity as a Competitive Advantage

According to Kosutic and Pigni (2021) top management "still view cybersecurity as a purely IT problem" (p. 28). Authors conducted a study by exploring "the impact of cybersecurity practices on competitive advantage" (p. 28) and based on this study, they proposed "Cybersecurity Competitive Advantage Model (CCAM) as a strategic framework to guide top management in building a competitive advantage" (p. 28).

But what is competitive advantage? According to Porter (1985) there are three generic strategies to achieve competitive advantage: 1) Cost leadership ("to become the low-cost producer"), 2) Differentiation ("to be unique") and 3) Focus ("selecting segment or group") which to target above all else (pp. 12-15).

In Cybersecurity Competitive Advantage Model (CCAM) competitive advantage is achieved by using differentiation strategy and it’s based on "building operational capabilities through holistic cybersecurity management" and "building cybersecurity

dynamics capabilities" (Kosutic & Pigni, 2021, p. 30). They state that "a company must create dynamic capabilities that are unique and difficult to copy" (Teece as cited in Kosutic & Pigni, 2021, p. 30).

### 2.2.2 Governance of Cybersecurity Management

Rajan et al. (2021) conducted a study which aimed to identify different factors that are affecting to organizations cybersecurity by using modified total interpretive structural model (p. 1). M-TISM is defined as an "advanced qualitative modeling technique which has been widely used" (Dhir et al., 2020; Haleem et al., 2012; Srivastava & Sushil, 2013; Wasuja et al., 2012 as cited in Rajan et al., 2021).

Their study was divided to 9 steps starting from identifying the factors and ending for constructing M-TISM model (Rajan et al., 2021, p. 5). Factors that they identified were “information flow, security awareness, technological infrastructure, resources and capabilities, training, alliance and collaboration, and governance” based on the literature review (Rajan et al., 2021, p. 7).

According to Rajan et al. (2021) findings was that governance "can be considered the most important factor in cybersecurity management, followed by alliances and collaborations" (p. 8). According to Rajan et al. (2021) "governance enhances the cybersecurity strategy by sharing knowledge, resources, experience and management support" (p. 10) but like the authors stated, in this study there were no empirical data used (p. 14).

### 2.2.3 Cybersecurity Legislation and the Fear of Severe Penalties

On April 26, 2016, European Parliament and the Council of European Union announced the General Data Protection Regulation (GDPR) 2016/679 which gives rights to the consumers and responsibilities to the organizations. GDPR also presented severe penalties for organizations that fail to comply with the regulation. According to article

83, penalties up to 20 million euros or up to 4% of annual worldwide turnover can be given (The General Data Protection Regulation, 2016).

In the United States, the Consumer Data Protection Act (CDPA), introduced by Senator Ron Wyden was "proposing jail time of up to 20 years for executives who knowingly sign off on incorrect and inaccurate annual certifications of their companies' data practices" (Wolff as cited in Chatterjee, 2019). Same bill also would have made possible to fine organization up to 4% of "annual revenue" which is like GDPR (Chatterjee, 2019, p. 1).

### 2.2.4 Cyberinsurance as a Cybersecurity Management Strategy

Cyberinsurance is defined as an insurance class which protects organisations for different kind of cybersecurity risks, and which is predicted to be growing market in the insurance business towards 2025 (Rudden, 2022).

Ogbanufe et al. (2021) conducted a study of top management's "commitment to use cyberinsurance" as cybersecurity management strategy (p. 1). Traditionally, organisations manage risks by using four different strategies: 1) risk mitigation, 2) risk acceptance, 3) risk avoidance and 4) risk transfer (p. 1). From these four, one way to manage cybersecurity risks is cyberinsurance which is the risk transfer approach (p. 1) but only to protect companies from "financial impact of a cybersecurity breach" (p. 1).

According to Ogbanufe et al. (2021) "choosing a cyberinsurance is a strategic decision" (p. 1) and many organisations have made this strategic decision. According to survey conducted in 2018, 75% of organisations has a cyberinsurance (Rudden, 2022).

### 2.2.5 Using Cybersecurity as a Strategic Asset

According to Hepfer and Powell (2020) companies that "have successfully managed through cyberattacks" see cybersecurity as a “top-level strategic priority" and not only operational thing. They have started to see cybersecurity as an "opportunity rather than

an expense" (pp. 40-41). Top-management have changed their perception from "operational to strategic, from reactive to proactive, and from threat-driven to opportunity-driven" (p. 42).

Hepfer and Powell (2020) argues "that organizational resilience requires four strategic capabilities: protecting the business, broadening awareness, managing consequences, and responding and recovering" (p. 43) which "allow executives to identify strategic opportunities" (p. 45). Overall, the finding of their study was that "resilience to cyberattacks requires advanced capabilities in all four elements of the model" (p. 45).

### 2.2.6 Strategic Cyber Intelligence to Support Decision Making

According to Borum et al. (2015) "intelligence is a key component" in cybersecurity (p. 317). Authors argue that simply the investments to the technology and systems are not enough but that added "cyber intelligence emphasizes prevention and anticipation" (p. 317). Idea is based on US Defense Science Board's Tasks Force on Resilient Military Systems and the Advanced Cyber Treat recommendation to "refocus intelligence collection and analysis to understand adversarial cyber capabilities, plans, intentions, and to enable counterstrategies" (DoD Defence Science Board as cited in Borum et al., 2015, p. 318).

Cybersecurity can be divided to: Strategic, operational, and tactical levels in which tactical level focus seems to be dominating factor in cyberdefence while strategical and operational levels "receive less attention" (Borum et al., 2015, p. 318). Strategic level is about "planning and control focuses on establishing an organization's mission and direction, setting objectives and conceiving plans for how those objectives will be achieved" (Mattern et al. as cited in Borum et al., 2015, p. 319).

According to Borum et al. (2015) cyber intelligence that is conducted in strategic manner can minimize organizational risks.

### 2.2.7 Strategically Motivated Advanced Persistent Threat

Advanced persistent threat (APT) is defined as well-educated technology specialists who have a funding. They usually operate in ordered manner and can use wide-range of different tools to conduct their missions (Hutchins et al.; Maisey; Mansfield-Devine as cited in Ahmad et al., 2019). Strategically motivated advanced persistent threat (S-APT) is defined as entities that are either criminal organisations, professional national hackers or organisations that are competing with the target organization (Ahmad et al., 2019).

Types of cyber threat agents by Ahmad et al. (2015) in hierarchical order:

1. Accidental (careless employee)
2. Malicious (script kiddies, disgruntled employees)
3. Organized (hacktivists, insiders)
4. Highly Sophisticated APTs (hackers engaging in criminal activity)
5. Strategically motivated advanced persistent threat S-APTs (professional hackers) (p. 407).

According to Ahmad et al. (2019) conquering advanced persistent threat requires knowledge that APT is a mission against the organization. Authors argue that systematically figuring out how advanced persistent threats (APTs) conduct their cyberattacks makes it possible to prevent these attacks.

Mostly offensive countermeasures such as direct targeting to them can't be used against S-APTs because legal boundaries but one way to prevent S-APTs by using lawful methods is to use disinformation against them. Especially giving them false information about IT infrastructure (Ahmad et al., 2019).

### 2.2.8 Strategy Role: IT Modernization vs. Legacy IT Systems

According to Pang and Tanriverdi (2022) "many organizations run their business operations on decades-old legacy IT systems" and "some security professionals argue that legacy IT systems significantly increase security risks" (p. 1).

There are currently two schools in IT modernization vs. legacy IT systems security debate. Other one thinks that legacy IT systems has more vulnerabilities and are not secure by design while other ones think that legacy IT systems are antique (security-by-antiquity) which lacks prober documentation and understanding of how these systems work (Pang & Tanriverdi, 2022, p. 4) which provides some forms of security.

In their study Pang and Tanriverdi (2022) proves that legacy IT systems "significantly increases the frequency of security incidents" (p. 14).

### 2.2.9 Strategic Approach for Nations Cybersecurity

According to Galinec et al. (2018) "cybersecurity has been practiced in military circles for over a decade" (p. 273). National cybersecurity is defined as a large concept that contains "policies, trainings, controls, configuration, encryption, anti-malware, boundary defenses, monitoring, vulnerability assessment, data recovery, incident response, threats and threat actors" (p. 275)

One of the approaches that authors present in their study is "people-centric security (PCS)" which is defined as "strategic approach to information security that emphasizes individual accountability and trust and de-emphasizes restrictive, preventative security controls" which is defined as alternative to "conventional control-centric approach" (p. 275).

According to Galinec et al. (2018) "government has a major role to play in stimulating progress toward higher levels of cybersecurity" and "operations-focused approach is needed" (p. 285). In national level and military terms, strategy is defined "utilization of all of a nation's forces" to "ensure security or victory". Authors argue that cyberstrategy defined by a nation can give the public and the private organisations a direction how they should conduct their cybersecurity activities (p. 278).

Authors argue that "national cybersecurity strategy should leverage the strengths of the government to drive evolution of the standard security practices used by government agencies, businesses and citizens in their daily use of cyberspace" (p. 278).

### 2.2.10 Cybersecurity Awareness Training as a Strategic Choice

According to He et al. (2020) "organizations ability to successfully manage intellectual capital is determined by the actions of its employees to prevent or minimize information security risks" (p. 203). They argue that "people are the weakest link in an organization's cybersecurity chain" (p. 204) and that the "organizations should provide cybersecurity awareness programs for employees at all levels" (p. 209).

He et al. (2020) conducted a survey which results founded that "the training methods do not have strong impact on employees' perceived severity, perceived benefits and response efficacy" (p. 209) but they do state that "organizations should continue their cybersecurity training" (p. 209) like updating systems, organizations employees must also be updated in the field of cybersecurity (p. 209).

He et al. (2020) continues to argue that "organizations must promote continuous education and training to employees on best practices for cybersecurity" (p. 210) but they also state that "a lot of cybersecurity awareness training is not effective" (p. 210). They recommend that organizations should "develop training materials with self-relevant information for future cybersecurity training of their employees" (p. 211).

## 2.3 Cybersecurity Management Standards and Frameworks

In this section, information security management standards and frameworks will be presented. These are not all standards and frameworks related to information security management but most essential, most used, and overall related to this research.

### 2.3.1 NIST Cybersecurity Framework

US National Institute of Standards and Technology (NIST) published a NIST Cybersecurity Framework. Current version 1.1 was published in April 2018 while the version 1.0 was published in February 2014 (NIST, 2022). NIST Cybersecurity Framework is available for multiple languages.

NIST Cybersecurity Framework is defined as being a cybersecurity management tool and it contains three components:

1. Core of the framework
2. Implementation tiers of the framework
3. and profile of the framework

(NIST, 2018, pp. 3-4).

#### 2.3.1.1 Core of the NIST Framework

*Core of the NIST framework* contains different things that organisations should do to achieve their objectives concerning cybersecurity. The core of the NIST framework is divided to four shown in Table 3. One is about functions, one is about categories and two others are about subcategories and references (NIST, 2018, p. 6).

Functions are divided to five: "Identify, Protect, Detect, Respond, and Recover" while categories are defined as "the subdivision of a function" and subcategories as the subdivisions of a categories, and informative references which are defined as "standards, guidelines and practices" which "achieve to the outcomes associated with each subcategory" (NIST, 2018, pp. 6-7)

| **Functions** | **Categories** | **Subcategories** | **Informative References** |
|---|---|---|---|
| Identify | | | |
| Protect | | | |
| Detect | | | |
| Respond | | | |

| | | | |
|---|---|---|---|
| Recover | | | |

**Table 3.** Researcher's illustration of the framework core.

#### 2.3.1.2 Implementation Tiers of the NIST Framework

*Implementation tiers of the NIST framework* are defined as to present how individual organization see their risk management approach (NIST, 2018, p. 8). Implementation tiers are dived to four tiers based on how sophisticated cybersecurity risk management practices organization use:

1. Partial
2. Risk Informed
3. Repeatable
4. Adaptive

(NIST, 2018, pp. 8-10).

| **Tiers** | **Risk Management Process** | **Integrated Risk Management Program** | **External Participation** |
|---|---|---|---|
| **1. Partial** | - Informal<br>- Managed reactively<br>- Prioritization is not connected to organizational risk objectives | - Limited awareness on the organizational level<br>- Cybersecurity risk management irregular | - Seeing things in bigger picture is not used<br>- Collaboration is not used |
| **2. Risk Informed** | - Approved by management<br>- No organizational-wide policy<br>- Prioritization is connected to organizational risk objectives | - Awareness of cybersecurity risk at organizational level<br>- Organization-wide approach not implemented<br>- Information is shared on informal basis | - Understands its role in the larger ecosystem<br>- Collaborates but not necessarily share information |

| | | | |
|---|---|---|---|
| **3. Repeatable** | - Formally approved<br>- Expressed as policy<br>- Practices regularly updated | - Entire organization is involved<br>- Organization has defined management practices<br>- It monitors cybersecurity risks | - Organization is a part of the bigger picture and may contribute to the community<br>- Collaborates with others and shares information with others |
| **4. Adaptive** | - Adapts practice based on current and previous activities<br>- Continuous improvement<br>- Advanced cybersecurity technologies and practices<br>- Respond in timely and effective manner | - Organization-wide approach<br>- Senior executives monitor cybersecurity risk<br>- Business units implement executive vision<br>- Part of organizational culture | - Organization is a part of the bigger picture and the community<br>- Organization does use information sharing<br>- Information shared is timely and relevant |

**Table 4.** Illustration of the implementation tiers.

Source: (NIST, 2018, pp. 8-10).

#### 2.3.1.3 Profile of the Framework

*Profile of the framework* is defined as to exist when core of the framework is in harmony with other things of the organization such as its business activities (NIST, 2018). Profile of the framework makes it possible that organizations can align their organizational goals, regulatory requirements, and best practices. Organization can have multiple profiles (NIST, 2018,).

Overall NIST Cybersecurity Framework is defined as "systematic process for identifying, assessing, and managing cybersecurity risk" and it is intended for "cybersecurity risk management tool" (NIST, 2018, p. 13).

### 2.3.2 ISO/IEC 27001/27002 - Information Security Management System

ISO/IEC 27001:2013 is defined as "the international standard for information security management systems (ISMS)" while ISO/IEC 27002 "can help organizations meet all their information-related regulatory compliance objectives" (Calder, 2013, p. 5). ISO/IEC 27001:2013 is about specifications while ISO/IEC 27001:2013 is about "code of practice" (Calder, 2013, p. 5).

#### 2.3.2.1 ISO/IEC 27001:2013

Like NIST Cybersecurity Framework, IOS/IEC 27001:2013 is also a systematic way to identify and manage cybersecurity risks that organization might face (Calder, 2013). It is defined as vendor-neutral and technology independent information security management system and can be applied to all kind of organizations (Calder, 2013, p. 13).

#### 2.3.2.2 ISO/IEC 27001:2013 and ISO/IEC 27000 Family

ISO/IEC 27002:2013 is defined as "code of practice for information security management" (Calder, 2013, p. 13). There is also other ISO/IEC 27000 family standard for information security, such as ISO/IEC 27003 which is implementation guide, ISO/IEC 27004 which is about measurement, ISO/IEC 27005:2011 which is about information security risk management and ISO/IEC 27006:2011 which is about audit and certification (Calder, 2013, pp. 13-14).

### 2.3.3 CIS Critical Security Controls (CIS Controls)

CIS Critical Security Controls is about best practices for computer security. It was earlier known as SANS Critical Security Controls (CIS, 2022). Current version is 8 which contains 18 controls:

1. First control is about assets management
2. Second control is about software related matters
3. Third control is about protecting organizations data
4. Fourth control is about security configuration
5. Fifth control is about account management
6. Sixth control is about access management
7. Seventh control is about vulnerability management
8. Eight control is related to audit logs
9. Ninth control is for mail and browsing
10. Tenth control is against malicious software
11. Eleventh control is how to act in case of data loss
12. Twelfth control is about network management
13. Thirteenth control is about how to network is monitored and protected
14. Fourteenth control is about cybersecurity related education
15. Fifteenth control is about how to management of SPs
16. Sixteenth control is how to manage security of the applications
17. Seventeenth control is about incident management
18. Eighteenth control is about pen testing

(CIS, 2022).

### 2.3.4 Payment Card Industry Data Security Standard (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is one information security frameworks worth mentioning. It is about security of the payment data. Current version is 4.0, published in March 2022 (PCI Security Standards Council, 2022).

#### 2.3.4.1 12 Principal Requirements

PCI DSS was originally created to ensure that paying with different cards is secure and to spread similar practices across the world (PCI Security Standards Council, 2022). PCI DSS contains 12 principal requirements:

1. "Install and maintain network security controls
2. Apply secure configurations to all system components

3. Protect stored account data
4. Protect cardholder data with strong cryptography during transmission over open, public networks
5. Protect all systems and networks from malicious software
6. Develop and maintain secure systems and software
7. Restrict access to system components and cardholder data by business need to know
8. Identify users and authenticate access to system components
9. Restrict physical access to cardholder data
10. Log and monitor all access to system components and cardholder data
11. Test security of systems and networks regularly
12. Support information security with organizational policies and programs"

(PCI Security Standards Council, 2022, p. 1).

In PCI DSS, each of the 12 principal requirement is described in very detailed manner containing multiple sections, overview descriptions, requirements and testing procedures and guidance (PCI Security Standards Council, 2022).

### 2.3.5 ENISA National Capabilities Assessment Framework (NCAF)

European Union Agency for Cybersecurity (ENISA) has published National Capabilities Assessment Framework (NCAF). Framework contains "17 strategic objectives" and is divided to 4 clusters:

1. Cluster 1: Cybersecurity governance and standards
2. Cluster 2: Capacity-building and awareness
3. Cluster 3: Legal and regulatory
4. Cluster 4: Cooperation

(Enisa, 2020, p. 8).

#### 2.3.5.1 Summary of Clusters

Cluster 1: Cybersecurity governance and standards is about developing national cyber contingency plan, establishing baseline security measures, and securing digital identify with building trust to the digital public services (Enisa, 2020, p. 8).

Cluster 2: Capability-building and awareness is about organizing exercises related to cybersecurity, establishing incident response capabilities, raising user awareness,

strengthening education, fostering research and development, providing incentives to the private sector, and improving supply chain cybersecurity (Enisa, 2020, p. 8).

Cluster 3: Legal and regulatory is about protecting critical information infrastructure, addressing cybercrimes, establishing incident reporting, and reinforcing privacy, and data protection (Enisa, 2020, p. 8).

Cluster 4: Cooperation is about establishing public-private partnerships, institutionalizing cooperation in public agencies and engaging to international cooperation (Enisa, 2020, p. 8).

Each cluster which contains multiple strategic objectives is furthermore divided to multiple individual goals (Enisa, 2020, p. 12).

#### 2.3.5.2 Maturity Levels

NCAF's goal is to "measure the maturity level of the cybersecurity capabilities of the Members states". In NCAF's, maturity is described in five different levels:

1. Level 1: Initial/Ad hoc
2. Level 2: Early definition
3. Level 3: Establishment
4. Level 4: Optimization
5. Level 5: Adaptiveness

(Enisa, 2020, p. 19).

Starting from maturity level 1 where nation has no "defined approach for cybersecurity capacity-building" and ending to maturity level 5 where nations "cybersecurity capacity-building strategy is dynamic and adaptive" (Enisa, 2020, p. 19).

According to Enisa (2022) NCAF can be used to evaluate nation cybersecurity capabilities, understand what maturity level country is, where the country can improve and to build cybersecurity capabilities.

# 3 Results

This chapter is about research description, data collection and analysis. Chapter will give a brief description about this research, how data collection was conducted and what were the limitations and delimitations for this study, followed by analysis.

## 3.1 Research Description

This research is about strategic cybersecurity management in organisations. Firstly, it explores the current situation in the field strategic cybersecurity management from the scientific literature. Secondly, it uses both, scientific literature, and collected secondary data to analyze current situation in the field strategic cybersecurity management to understand fields current situation better. Based on the analysis, final intention of this research is to develop conceptual model for the strategic cybersecurity management which can be used in all types of organisations, or even individuals alone to improve their strategic cybersecurity management.

## 3.2 Data Collection

Literature review which is the foundation of the theoretical framework of this research, is based on peer-reviewed scientific articles in the field of strategic cybersecurity management by relevance and by using keywords "strategic cybersecurity management". Focus on this research is the latest scientific research contributions. Books that were used in this research were based on known authors in the field of strategic management.

Secondary data collection is mainly used to save time and for convenience reasons to make this research much more effective based on the timeline and the scope of this research. Secondary data is used in analysis to present trends, amounts, and current situations in the field of strategic cybersecurity management. Primary data collection is used in comparative analysis to compare if used secondary data aligns with primary data.

Comparative and descriptive analysis mainly used to analyze results. Comparative analysis is used to present differences in measurement while descriptive analysis is used to present similar or different perspectives or opinions based on the arguments.

### 3.2.1 Limitations and Delimitations

Potential weaknesses that this research contains are location based (e.g., country based) research results. Because this research uses mainly secondary data collection, study is limited to availability of research contributions of other researchers. Study will use data what is currently available and can be implemented to this research. Based on the other limitations such as thesis work time constraint which researcher has no control of. This thesis is summarized study of the strategic cybersecurity management limited to these outside enforced constraints.

What comes to delimitations, I have decided to include most recent studies in the field of strategic cybersecurity management and exclude the older studies. I have also decided to include cybersecurity frameworks which are mainly used by United States based companies and exclude cybersecurity framework which are mainly used by European or worldwide companies because availability of the research data. There is no or I couldn't find any cybersecurity framework adoption studies that are related to only European countries, or which are related to companies operating worldwide but many of the larger United States based companies are also companies that are operating worldwide, both in Europe and elsewhere.

## 3.3 Strategic Cybersecurity Management

This section is about analysis of the recent research focus in the field of strategic cybersecurity management. Where to scientific research focus has been lately? What has been studied recently? and what we can learn about it?


**Figure 4.** Recent scientific research focus based on literature review.

Based on the literature review in section 2.2 Strategic Cybersecurity Management, I have founded out that there are 10 different categories where recent scientific research focus in the field strategic cybersecurity management has been based on relevance as shown in figure 4.

### 3.3.1 Analysis: Cybersecurity as a Competitive Advantage

I would presume that most would agree to direction of Kosutic and Pigni (2021) study about helping top management to achieve competitive advantage in cybersecurity (p. 28) and there seem to be supporting evidence for taking this step. United States based worldwide technology company Apple Inc. seem to have taken this direction. According to Apple (2022) they see one cybersecurity area, privacy as a "fundamental human right" and they have implemented this view to their company's core values.

One way to achieve competitive advantage in cybersecurity is "to be unique" which is called differentiation strategy (Porter, 1985, pp. 12-15) and not only to be unique but to be also "difficult to copy" (Teece as cited in Kosutic & Pigni, 2021, p. 30). Apple Inc. seem

to use this differentiation strategy to achieve their uniqueness in field of cybersecurity by utilizing security layers, security controls, hide protections, tracking transparency, "intelligent tracking preventions", history controls and many other privacy and security controls and services to their products and services (Apple, 2022). At least with to success that their products and services seem to be more secure (Doffman, 2021). Are they? That's a whole another study. But the direction to use cybersecurity as a competitive advantage seems to be useful, in the world where we all are one way or another vulnerable to different kinds of cyber threats?

### 3.3.2 Analysis: Governance of Cybersecurity

According to Rajan et al. (2021) governance, alliances and collaborations are the three main factors in cybersecurity management from which governance is the most important (p. 8). Governance is defined as "act or process of governing or overseeing the control and direction of something" (Merriam Webster, n.d.) or "the way that organizations or countries are managed at the highest level, and the systems for doing this" (Cambridge Dictionary, n.d.).

Rajan et al. (2021) is not alone with their finding that governance is the most important factor in cybersecurity management (p. 8). According to Yusif and Hafeez-Baig (2021) scientific literature has also many times "emphasized the importance of the implementation of cybersecurity governance" (p. 491) to protect organisations IT. Maleh et al. (2021) took this to step further by proposing a "maturity framework for cybersecurity governance" called CYBERGOV Framework (p. 7) where both, the strategy, and the governance together to "provide the oversight structures for supporting CYBERGOV" (p. 8). Can we counter-argue against to importance of cybersecurity governance? I would presume that cybersecurity governance is important.

### 3.3.3 Analysis: Cybersecurity Legislation and the Fear of Severe Penalties

After the General Data Protection Regulation (GDPR) 2016/679 made possible to give severe penalties to organisations which does not comply with to regulation, here's the highest GDPR fines issue to this day shown in Table 5 below.

| Date | Organisation | Amount | Issue by | Source |
|---|---|---|---|---|
| 2021-06-16 | Amazon Europe Core Sarl | €746,000,000 | Luxembourg | (Metha & Chee, 2021) |
| 2021-09-02 | WhatsApp Ireland Ltd | €225,000,000 | Ireland | (Data Protection Commission, 2021) |
| 2019-07-08 | British Airways | £183,000,000 | United Kingdom | (BBC, 2019) |

**Table 5.** Highest GDPR fines issued to this day.

Just by looking the pure numbers of these highest GDPR fines, there's no wonder why top management see cybersecurity as one of the biggest concerns to their business (Kosutic & Pigni, 2021, p. 28) and why some researchers point out that "cybersecurity is a serious issue" (Rajan et al., 2021, p. 120872). Based on the amounts of the fines, obviously cybersecurity can be seen as a very serious matter.

### 3.3.4 Analysis: Cyberinsurance as a Cybersecurity Management Strategy

According to Johnson (2021) average cost from the data breach for organisation in the United States was 8.64 million dollars in 2020 and it is showing a growing trend as shown in figure 5 below.

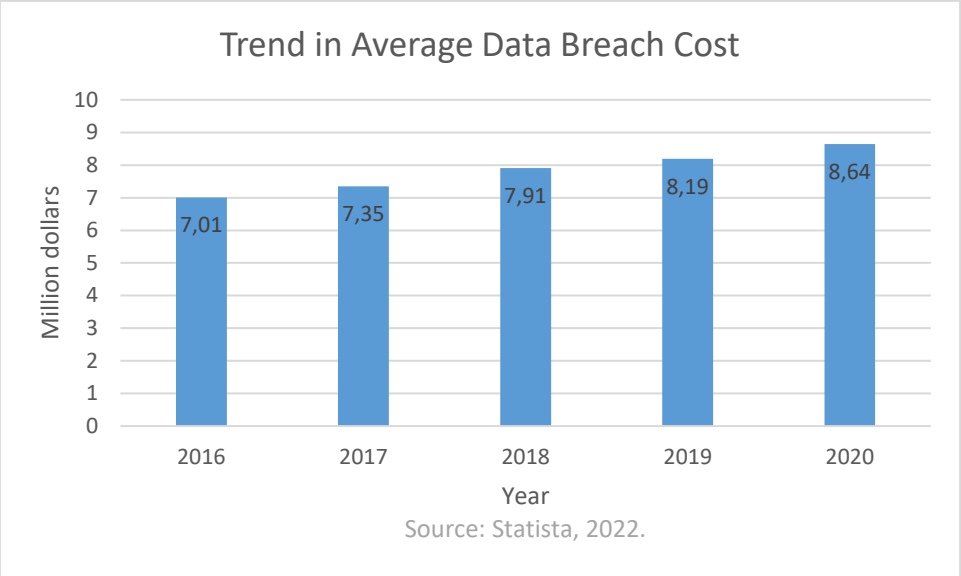


**Figure 5.** Trend in average data breach cost in the United States 2016 to 2020.

We can predict that if costs of data breaches are increasing, also possible cyberinsurance costs are increasing for the organisations. Cyberinsurance as a cybersecurity management strategy is a risk transfer approach in organizational risk management (Ogbanufe et al., 2021, p. 1) but it only covers possible financial losses of the data breach, and itself does not protect organisations from hacking attempts. Except insurance companies usually require some form of auditing before granting a cyberinsurance (Zhao et al., 2013, p. 130).

### 3.3.5 Analysis: Using Cybersecurity as a Strategic Asset

Based on the literature review, Hepfer and Powell (2020) along with others encourage to use cybersecurity as a strategic asset. Reagin and Gentry (2018) not only encourage but they state that cybersecurity is a strategic asset.

Allen and Cervo (2015) highlights to importance of the management of the strategic assets such as data. While data is usually one of those things that organisations cybersecurity practices protect, it's argued that top management "fail to recognize

cybersecurity as a strategic priority" (Hepfer & Powell, 2020, p. 41) and it is shown, according to Perry (2020) that only half of small businesses are prepared for cyberattack.

### 3.3.6 Analysis: Strategic Cyber Intelligence to Support Decision Making

There is no doubt that strategic cyber intelligence is also very important factor in strategic cybersecurity management. Based on the study "Strategic Cyber Threat Intelligence Sharing: A Case Study of IDS Logs" conducted by Dog et al. (2016), here's a list of top five countries in figure 6 from where cyberattack events originated by using strategic intelligence gathering.

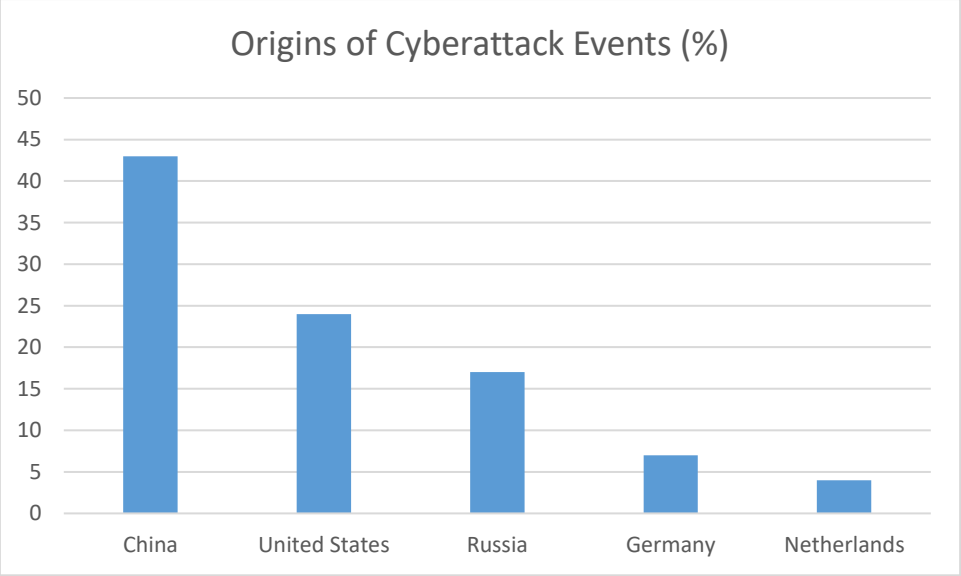


**Figure 6.** Origins of cyberattack events by country.

If I compare Dog et al. (2016) case study to my own IDS (Intrusion Detection System) logs from my website at www.janipaivarinta.com, I founded out that we both have same top five countries, but amount of cyberattack events are different as shown in figure 7.

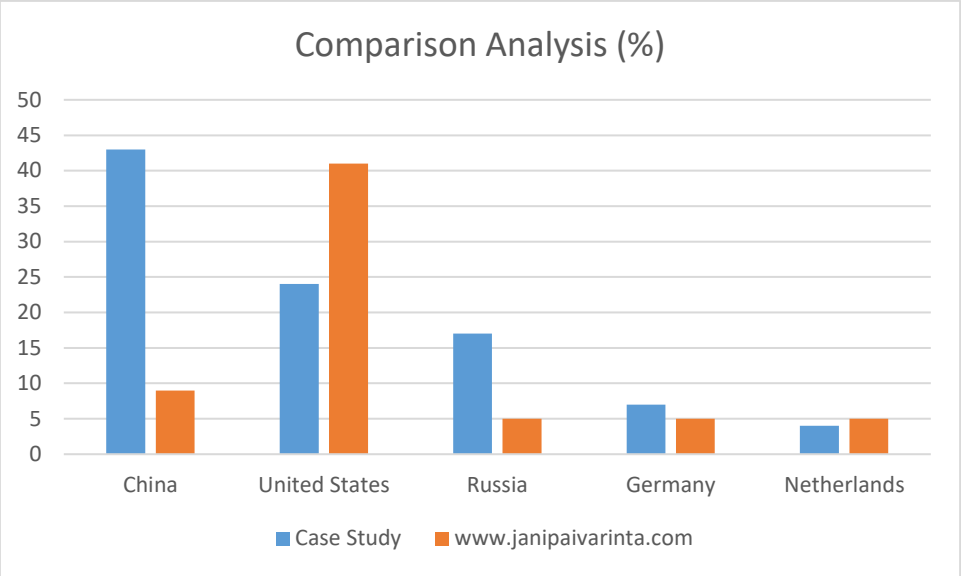


**Figure 7.** Comparison analysis of cyberattack events by country.

Dog et al. (2016) argue that sharing cyber threat intelligence (CTI) is "important tool" to "prevent attacks" and I couldn't agree more (p. 1). Just by comparing these two data sets, I have learned that top origin countries of cyberattacks events are same which highlights to importance of strategic cyber intelligence information sharing.

### 3.3.7 Analysis: Strategically Motivated Advanced Persistent Threat

According to Rieder (2022) worldwide cybersecurity companies have identified about 150 APT groups. How many of these APT groups would be identified as strategically motivated advanced persistent threat (S-APT)? That we don't know.

Many of these identified APT groups are associated with some countries such as China, Russia, Iran, North Korea, and Vietnam (Mandiant, 2022) but leaves out their western counterparts which have their own history of cyberattacks. One of them was known a malware attack called "Stuxnet" which was delivered to Iran, and it is widely speculated that United States and Israel was behind it (Nakashima & Warrick, 2012).

### 3.3.8 Analysis: Strategic Role: IT Modernization vs. Legacy IT Systems

In United States, based on the "State of IT Modernization 2020" report, current direction in IT modernization seems to be that majority of organisations are modernising their IT infrastructure and moving towards a public cloud (IDG, 2020). Half of the survey respondents stated that "managing public security is the #1 challenge in cloud optimizations" (p. 6). Direction is aligned with my own observations.

In Q4 2021, the biggest cloud providers were Amazon AWS, Microsoft Azure, Google Cloud, Alibaba Cloud, IBM Cloud, Salesforce, Tencent Cloud and Oracle Cloud as shown in figure 8 below (Richter, 2022).

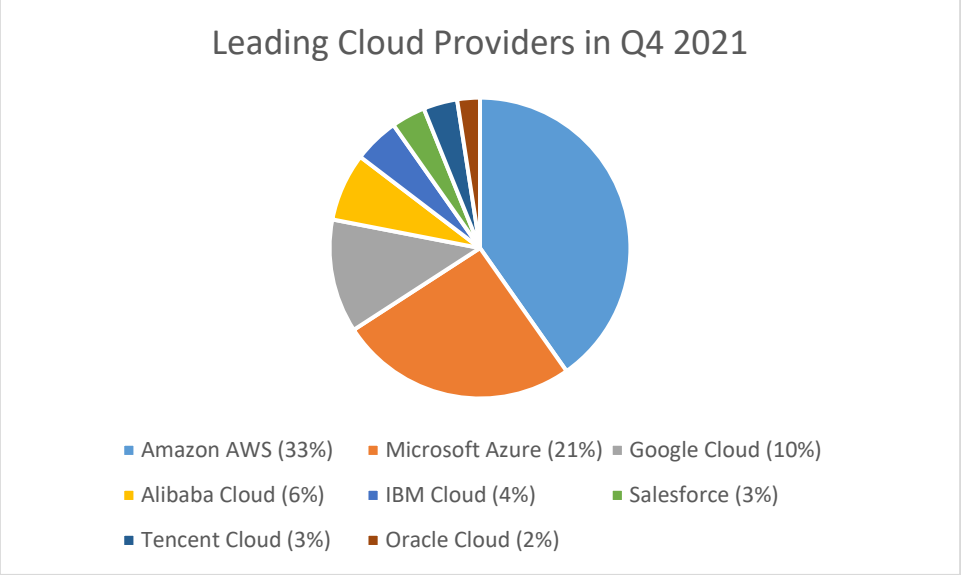


**Figure 8.** Leading cloud providers in Q4 2021.

But still according to IDG (2020) survey report, 64% of organizations engage to IT modernization seem to use hybrid cloud approach (p. 6).

### 3.3.9 Analysis: Strategic Approach for Nations Cybersecurity

According to UK Government's (2021) "Cyber Security Breaches Survey 2021" 39% of UK-based companies and 26% of UK-based charities reported to have cyberattack or cyber

security breach. Report detected three targets where these cyberattacks, and cybersecurity breaches has been higher in the past years and in the current year as shown in figure 9 below.

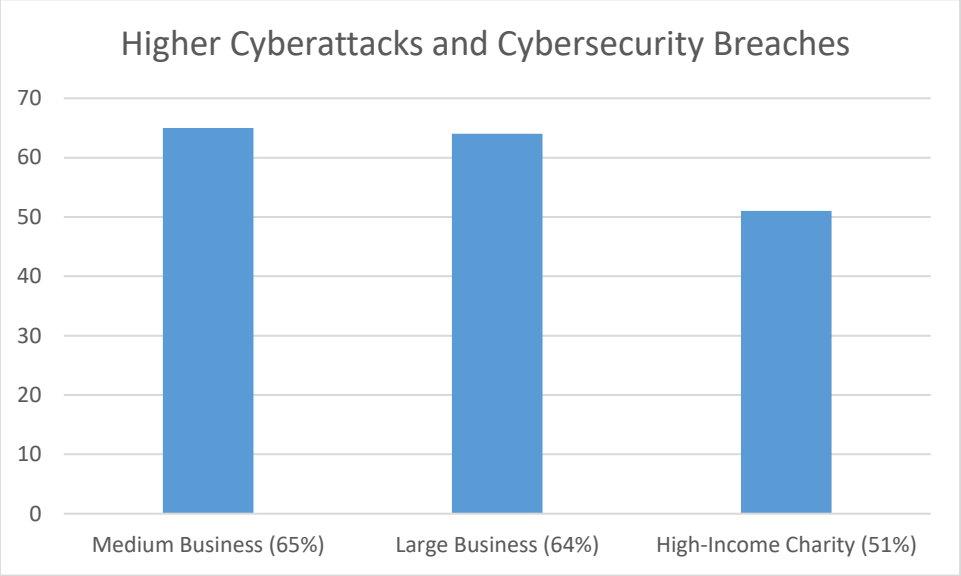


**Figure 9.** Higher cyberattacks and cybersecurity breaches.

Along with monitoring country's cyber incidents and setting goals "toward higher levels of cybersecurity" (Galinec et al., 2018, p. 285), why is nations involvement needed in organization cybersecurity? In June 2020, eBay's Senior Director, Director and multiple employees of eBay's security team were arrested in connection to cyberstalking campaign. All employees pleaded guilty, one got 18 months in prison while others are still waiting their sentence. Senior Director of Safety and Security pleaded guilty in April 2022 while Director of Global Resilience has pleaded not guilty (U.S. Attorney's Office, 2022).

But this was not a small harassment campaign. Their cyberstalking campaign included victim's surveillance, trying to deceive law enforcement officials, destroying evidence when spotted, fabrication of records and sending all kind of disturbing material to the victim's home along with many other very disturbing things (U.S. Attorney's Office, 2022). This was a case where Fortune 500 company (Fortune, 2022) including its senior

management were trying to weaponize the internet against a victim couple who criticized eBay (CBS Boston, 2020).

### 3.3.10 Analysis: Cybersecurity Awareness Training as a Strategic Choice

He et al. (2020) argues that the "people are the weakest link in an organisation's cybersecurity chain" (p. 204). In cyberattacks that has been successfully conducted against organisations, human error seems to be a root cause in 95% cases (InfoScales report as cited in Sharma, 2019). In Verizon (2021) "2021 Data Investigations Breach Report" (DIBR) human was involved in 85% cases.

According to Zuopeng et al. (2021) organisations need to conduct cybersecurity awareness trainings (CSATs) to minimize cybersecurity threats and one way to do it, is to improve employees' capabilities to detect cyber incidents and act in the face of cybersecurity threats.

## 3.4 Organisations Adoption of the Cybersecurity Frameworks

This section is about how organisation have adapted different kind of cybersecurity standards and frameworks.

### 3.4.1 Analysis: General Adoption of Cybersecurity Frameworks

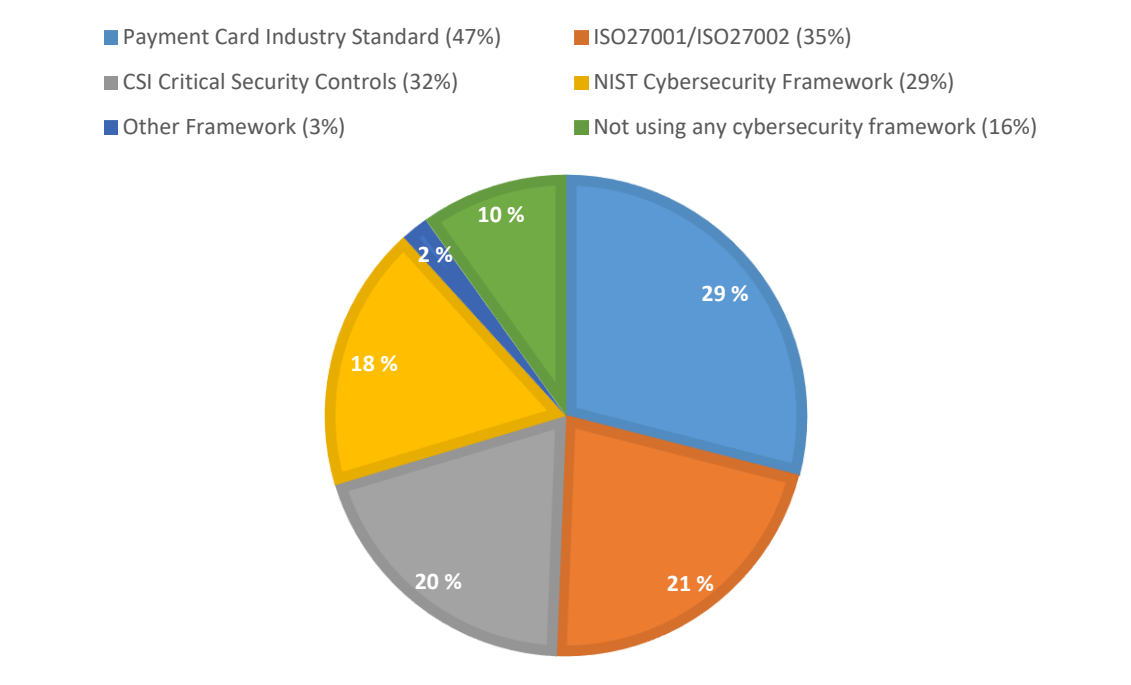


**Figure 10.** Cybersecurity framework adoption (Dimensional Research, 2016).

According to study "Trends in Security Framework Adoption" what was conducted in United States by Dimensional Research (2016), and which was "based on a survey of 338 IT and security professionals in the United States" (p. 2), 84% of companies are using some type of information security framework (p. 5). 44% of companies are using multiple cybersecurity frameworks (p. 2). Payment card industry (PCI) standard is used by 47% of companies, ISO27001/ISO27002 is used by 35% of companies, CIS Critical Security Controls is used by 32% of companies and NIST Cybersecurity Framework is used by 29% of companies while only 3% of companies are using some other framework and 16% of companies are not using any type of cybersecurity framework (p. 5).

### 3.4.2 Analysis: Adoption of Cybersecurity Frameworks by Industry

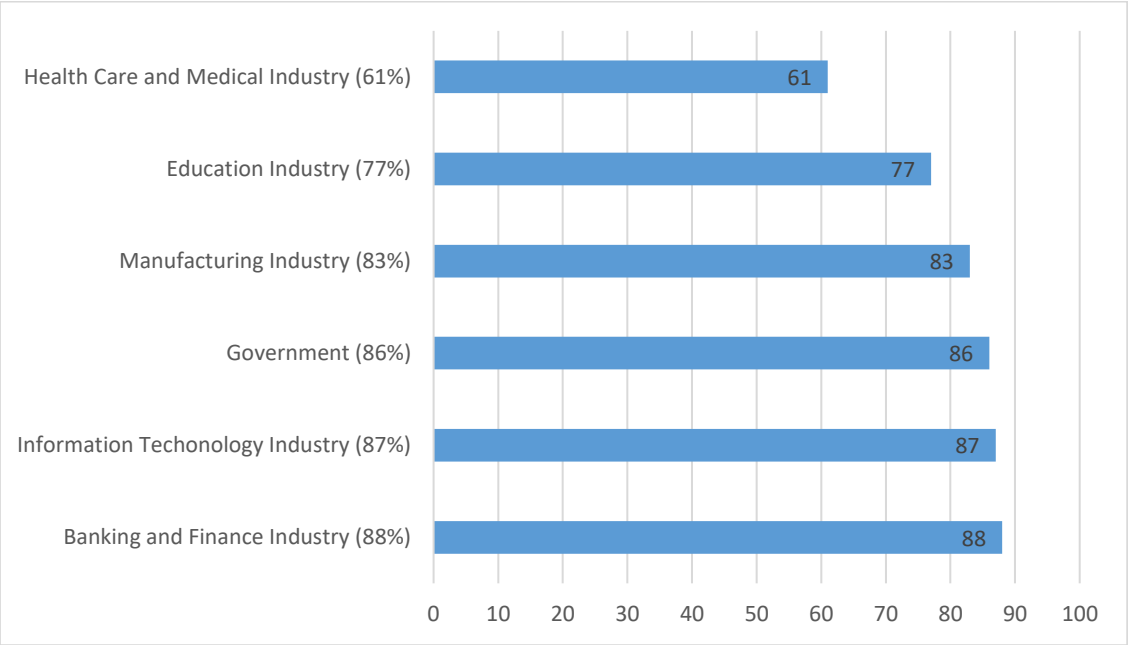


**Figure 11.** Framework adoption by industry (Dimensional Research, 2016).

Banking and finance industry was among the top performers of industries in cybersecurity framework adoption with 88%, followed by information technology industry close by with 87% and government with 86% adoption rate. Other industries were manufacturing with 83%, education sector with 77% and health care and medical industry with 61% adoption (Dimensional Research, 2016, p. 4).

### 3.4.3 Cybersecurity Framework Adoption Summary

While majority of organisations have adopted cybersecurity framework and almost half have adopted multiple cybersecurity frameworks, there still organisations that doesn't have adopted any type of cybersecurity framework (Dimensional Research, 2016).

According to Cieslak (2016) there are two main reasons which prevent organisations to adopt cybersecurity framework: 1) regulators might not require adoption of cybersecurity framework and 2) organisations must make heavy investments if they intend to adopt cybersecurity framework.

# 4 Discussion

Based on the literature review and analysis, this chapter is about proposing a new conceptual model for the strategic cybersecurity management which organisations can use to improve their existing strategic cybersecurity management. Conceptual model proposed in this chapter is based on the observations and findings of the earlier chapters along with researcher's empirical experience and surfaced improvement ideas.

## 4.1 Proposed Conceptual Strategic Cybersecurity Management Model

### 4.1.1 Structure of the Conceptual Model

Based on the literature review, analysis, observations, findings, empirical experience, and surfaced improvement ideas, I have found three strategic choices that organisations can make to improve their strategic cybersecurity management as shown in figure 12 below.

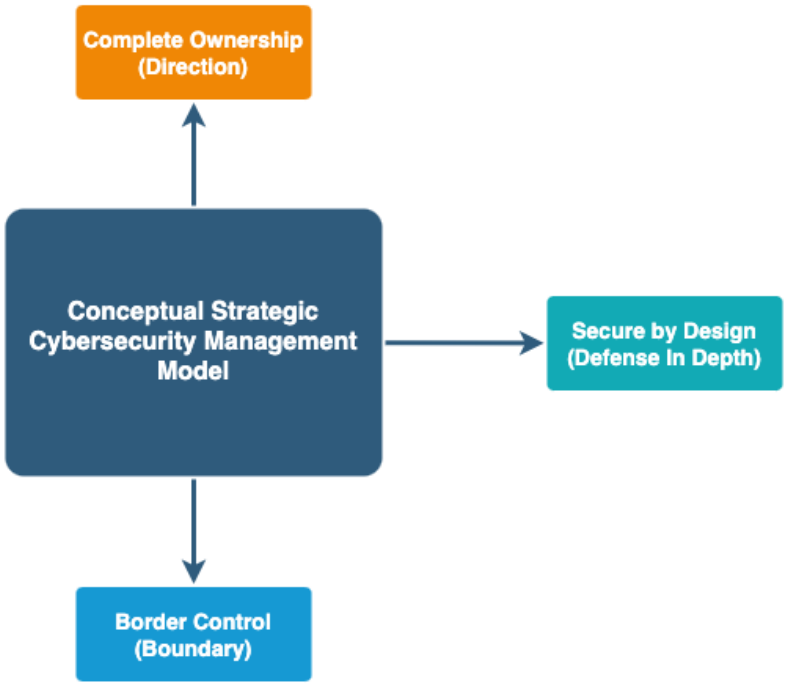


**Figure 12.** Conceptual strategic cybersecurity management model.

### 4.1.2 Strategic Choice 1: Complete Ownership

First proposed strategic choice is *complete ownership* which means that organisation should move from outsourcing to complete ownership. Taken to the extreme form, organisation would manufacture its own devices from processors to data storages, its own systems from operating systems to single applications and all its services from in-house mail servers to the external web services offered to the clients.

Strategic choice of complete ownership is about restoring control. When organisations outsource their IT functions to the third parties, they will lose control of their IT and when they lose control, they lose their ability to protect themselves. According to IDG (2020) report, majority of organisations are using public cloud infrastructure. These organisations have no physical access to their public cloud servers. They have no physical access to their public cloud storages which contains their data. I would presume that most organisations don't even know where their data is physically located. Not owning your IT systems means you have no control of your IT infrastructure.

### 4.1.3 Strategic Choice 2: Secure by Design

Second proposed strategic choice is *secure by design* which means that organisation should build its IT infrastructure and IT systems to be highly secure by default. In a practical level, this means that organisation will use encrypted in-house servers, distributes full-disk encrypted devices to its employees with strong password policy, has encrypted backups of their servers, employee devices and have overall security hardened IT infrastructure and IT systems, e.g., principle of minimal application (means that organisation devices contain only needed applications to minimize attack surface).

On January 28, 2022, Pilke (2022) reported that Ministry of Foreign Affairs of Finland diplomats were targeted by Pegasus spyware. Where Ministry of Foreign Affairs of Finland failed in this case was to secure their devices abroad. Ministry of Foreign Affairs of Finland didn't give any explicit information about the attack but according to Gurijala

(2021) Pegasus can be delivered to smartphone by using WhatsApp call or by sending a text message. Removing WhatsApp application or any application that has history of abuse (by using a principle of minimal application) and disabling text messages makes organisations devices more robust against these kinds of attacks.

### 4.1.4 Strategic Choice 3: Border Control

Third proposed strategic choice is a *border control* which means that organisation should establish border control to its IT infrastructure, IT systems and IT services. E.g., if organisations only market area is Finland and its only target customers are Finnish customers, its web services for clients should only be open for visitors from Finland. Keeping web service open to the entire world when it is not necessary minimizes ways that attackers can use to target specific organisation.

On April 8, 2022, Defence Ministry of Finland (2022) tweeted that their website defmin.fi is down because of the denial-of-service attack. Where Defence Ministry of Finland failed in this case was in use of border control. Most likely their website was open to entire world which made them vulnerable for these kinds of attacks. If they would have implemented proper border control, this kind of attack would not have any impact on them whatsoever. But Defence Ministry of Finland is not the only organisation that is completely open for denial-of-service attacks.

## 4.2 Execution of Conceptual Strategic Cybersecurity Management Model

This section is about examples how to successfully execute proposed three strategic choices in any type of organisation, big or small.

### 4.2.1 Example of Conceptual Model Execution

Figure 13 below shows one example how organisations could execute three strategic choices.

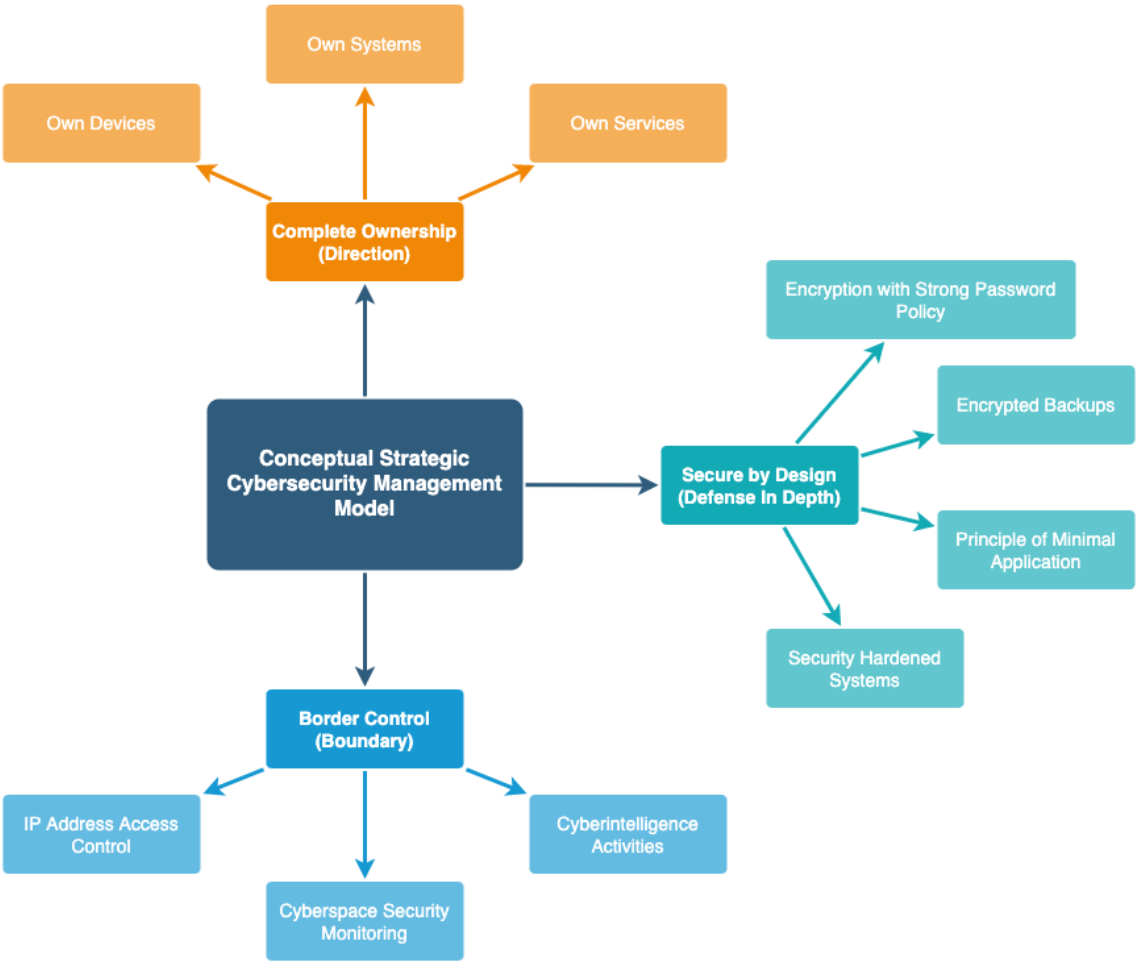


**Figure 13.** Example of conceptual model execution.

### 4.2.2 Strategy Execution Example 1: Complete Ownership

First the direction, complete ownership. From organisation current situation, organisation should move towards model where organisation owns everything in its IT infrastructure. This includes organisations servers which provide services for both internal and external clients. It also includes desktop computers, laptop computers and smartphones which organisation employees use to conduct their day-to-day tasks.

If BYOD (Bring Your Own Device) policy is implemented in organisation, complete ownership should be implemented on employees too. That means that employee who use their own device for work related tasks should own that device completely. That means that device, which is rented, or property of a third person cannot be used.

In a practical level, organisation should start to move from public cloud infrastructure towards privately own private cloud infrastructure by buying own servers, establishing physical security monitoring to their own server space, and starting to move their public cloud services to their own private cloud servers.

At the same time, organisations should start to move from IT-leasing to organisation owned devices or by implementing a BYOD culture with employee-owned devices. All this will increase organisations and its employee's ability to control their IT infrastructure. What more control organisation and its employees have over their IT systems that better they can manage cybersecurity related threats what they are facing is the argument.

### 4.2.3 Strategy Execution Example 2: Secure by Design

Secondly, secure by design. Most IT systems are not secure by design, e.g., if you buy an average home laptop from any store, it most likely uses Windows 10 or Windows 11 home operating system which is not encrypted at all. That laptop most likely also contain some additional bloatware installed by the laptop manufacturer. To make that single laptop suitable for organisations IT infrastructure, owner needs to change its operating system to Windows 10 Pro or Windows 11 Pro at least to get full-disk encryption which will protect organisations data assets in the case of theft. Same full-disk encryption should be used when organisation sets up its servers.

Encryption is usually 128-bits or 256-bits, one bit is 8 zeros or ones, or combination of zeros and ones. 128 divided by 8 is 16 and 256 divided by 8 is 32. That means that strong password policy for the organisation should be at least 16 characters or more which is not the case in many organisations. Most organisations that I have worked, have given me 8-character password which equals to 64-bit encryption. Laptop that has 128-bit full-disk encryption and 8-character login password, does not have 128-bit full-disk encryption, it has 64-bit full-disk encryption.

When organisation or its employees own their devices, they can modify or harden their devices without asking anyone's permission. They can remove unnecessary bloatware. They can even make additional hardware modifications if needed. They can only install applications that is needed in their organisation and get rid of the rest to minimize attack surface. They can implement other security controls to make their devices as secure as possible such as mandatory encrypted backups for both, organisations servers and employees' laptops. This way if something brakes, nothing has been lost in organisational or employee level. If organisation has BYOD policy implemented, these secure by design principles should also be enforced to employee-owned devices (full-disk encryption, min. 16-character password, encrypted backup, and other security hardening policies) with mutual agreement.

### 4.2.4 Strategy Execution Example 3: Border Control

Thirdly, border control. Now that organisation has its own IT infrastructure, own IT systems and most likely own IT services located in organisations facilities it's time to implement border control. It means limiting access to organisations IT infrastructure and systems from outside, both physically and in cyberspace. Border control of an IT infrastructure is like a border control of a country. Firstly, you have borders. Your borders can be crossed only with your permission and your border is guarded. In IT infrastructure this can mean limiting access to email server only from internal VPN connection. It can mean limiting access to client-side web services to only from geolocations that your organisation currently operates. If your organisation operates in all countries of the world, you could implement border control by positioning your servers to those countries that you operate and limiting access to that country's servers from that country only. In this way, if one location is attacked, all other locations will stay normally operational.

Simply limiting access to organisations IT systems is not enough. Border control also needs proper border guards which physically monitor, gather cyber intelligence, and make decisions concerning visitors who are trying the access to organisations systems

and services with malicious intentions. In practical level, this can mean having a cybersecurity team which responsibilities is to monitor your organisations IT infrastructure around the clock. In smaller organisation this can be done by an owner, each individual or it can be automated in some extent. Executing border controls just means that organisation has access controls in place, access is monitored and cyber intelligence from possible malicious actors are gathered to prevent any type of attacks before they occur.

# 5 Conclusions

This chapter is about summarizing the content, research contributions, assessment of reliability and validity, and possible future research. Chapter will summarize this research from title to final conclusions, describe research contributions and key results, evaluate research validity and reliability, and propose possible future research topics.

## 5.1 Research Summary

This research was about organisations strategic cybersecurity management. What was the current situation of the organisations strategic cybersecurity management based on the literature review and data collection? and how that situation could be improved so that organisations could move towards cybersecurity excellence?

Study started from understanding that cybersecurity is one of the biggest concerns of the top management because of cybersecurity threats are increasing all over the world and cyberattacks are ever more sophisticated in nature. To counter these cyber threats organisations must improve their current strategic cybersecurity management and take a direction toward cybersecurity excellence in organisations day to day activities.

This study was conducted by using extensive literature review to understand current scientific research focus and what kind of strategic management practices organisations use in their current strategic cybersecurity management context. Scientific literature review was extended by secondary data collection to understand numbers, quantities, and possible trends. Research was conducted by using mixed methods research approach where qualitative and quantitative research approaches followed each other to answer defined research questions: 1) What was the current situation of the organisations in the field of strategic cybersecurity management? and 2) What kind of models, frameworks, principles, and the practice we need to develop to achieve organisational cybersecurity excellence?

Literature review was the foundation for the theoretical framework of this research. Review identified 10 different strategies that organisations use in their strategic cybersecurity management which were: using cybersecurity as a competitive advantage, governance, cybersecurity legislation, cyberinsurance, cybersecurity as a strategic asset, strategic cyber intelligence, strategies against strategically motivated advanced persistent threat, IT modernization vs. legacy systems, nations strategic approach to cybersecurity and cybersecurity awareness training. Literature review was limited to recent scientific research by relevance and was followed by analysis.

In analysis, this research used scientific literature and secondary data collection to understand this topic and cybersecurity related matters better. Analysis included comparative analysis and descriptive analysis techniques. It provided better overall picture of the organisations strategic cybersecurity management by using both numbers and different perspectives.

Based on the literature review and analysis, this research identified three strategic choices that organisations can use to improve their strategic cybersecurity management. These proposed strategic choices were complete ownership, secure by design and border control. While current trend is towards public cloud IT infrastructure, complete ownership proposes completely controversial approach to change current trend direction towards private cloud IT infrastructure to improve cybersecurity. While current strategic cybersecurity management contains pieces of IT systems security this research proposes to go towards secure by design IT systems where encryption, even backing up employees' devices and devices security hardening plays a significant role. While most organisations are completely open for an attack from all over the world, this research proposed to implement tight border control which is comparable to border control of which different countries use to decide who can enter to their country and who cannot.

## 5.2 Research Contribution

This research proposes that by implementing these three presented strategic choices in this study: complete ownership, secure by design and border control will be three strategic choices that organisation can use in their journey towards a cybersecurity excellence.

Research does not exclude any other strategic cybersecurity management practices, choices, tools, or frameworks but provides three strategic choices to improve organisational strategic cybersecurity management. These three choices can be used by small or large organisations, even single individuals to improve their overall cybersecurity.

Three strategic choices were presented with execution examples to demonstrate abstract possibilities how these choices can be implemented. Complete ownership was about direction and which direction organisation should take to achieve cybersecurity excellence. Secure by design was about defence-in-depth and how organisations should protect their IT systems to achieve cybersecurity excellence. Border control was about using boundaries and how organisations should use boundaries to achieve cybersecurity excellence. All these three strategic choices together can help organisation to improve their overall cybersecurity.

This research provided current view for the organisational strategic cybersecurity management based on scientific literature, secondary data collection and analysis. This research also identified what kind of models, frameworks, principles, and the practices we need to develop to achieve cybersecurity excellence. Outcome of this research was three strategic choices which is a model, a small framework, three principles and three practices combined to achieve cybersecurity excellence.

## 5.3 Reliability and Validity

Literature review of this research was based on peer-reviewed scientific articles from scientific journals, few books from well-known authors in the field of strategic management such as Michael Porter. Data collection was based mainly on secondary data sources to save time and improve efficiency of this research but only to present amounts and quantities. Participant error or participant bias cannot be evaluated because of the nature of using secondary data. Primary data collection was used from researcher's source in comparative analysis to see similarities and to understand that data collected from different sources present similar trends (e.g., same top five countries where cyberattacks are coming from). From the researcher's perspective, this study was conducted as much objective standpoint view as possible.

Some of the secondary data was collected from research conducted in United States, focused on companies in the United States and does not necessarily have anything to do with European or worldwide research results but this research was constructed so that it can be replicated by using different data sources from Europe or worldwide. Would they have any influence on proposed strategic choices, not really. Proposed strategic choices were based on overall picture of the field and additional empirical experience of the entire field of strategic cybersecurity management and for that reason different numbers or trends would not have really changed to outcome of this research.

In the results chapter of this research, numbers, and quantities measure what they claim to measure, so construct validity should be there. All variables were presented in a simple and clear manner to withhold internal validity between two or more variables which clearly presents relationships between different variables. Based on the research findings, would external validators come to same conclusions? At least they should be making similar generalizations, so the external validity should be there.

This research was a master's thesis for the industrial systems analytics programme at University of Vaasa. Thesis work has a defined time constraint. This time limit which is

reserved for the thesis work defines how extensive this research can be. While this research was conducted in accordance with the time constraint, it proposed outcomes: three strategic choices that can be implemented by any individual or any public or private organisation to improve their cybersecurity. Outcome from this research can be generalized for everyone who needs or wants to improve cybersecurity of their information systems such as servers, computers, smartphones, tablets, IoT devices and others.

## 5.4 Future Research

What further research topics from this research arise? Strategic cybersecurity management is large, complex, and multi-disciplinary field. Its combines strategic management, financial management, information management, information and communication technologies, military science, and many other fields of expertise. While it is highly technical field because its intention to protect organisations from different kind of cyber threats which can come to organisations by using signals, systems or networks, there are plenty of future research topics in this field.

Main concern that arises from this research is that organisations cybersecurity is not very-well organized, managed and executed at least in strategical level. Current scientific research is focused on the small things or small parts of cybersecurity but the big things or essential strategic level decision that will guide organisations towards cybersecurity excellence are not very well conducted. Maybe one of the future studies would be to understand current situation of the top executives understanding about cybersecurity matters. At the current moment, it seems that organisation have done something to prevent cyber threats either by based on regulatory requirements or by voluntary actions, but organisations are not well prepared to encounter cyberattacks. Single government or country also lacks abilities to stop cybercrimes mostly because they are not originated from the place where country has a juridical authority, and this puts organisations in situation where they need to take larger responsibility of their cybersecurity matters. Countries will not protect organisations, and law enforcement

officials doesn't necessarily have means to capture cyber criminals originated from another country or out of their jurisdiction.

Another future research topic which arises from this research is to examine how many cybercrimes different organisations have faced in the past years and how many of those law enforcement officials was able to investigate and forward to prosecution. It would be interesting to see percentages of captured and non-captured cyber attackers. There is also room to do more extensive and precise study from where cyberattacks are mainly originated, what type of cyberattacks are mostly used and maybe examine motivations behind the different kind of cyber attackers.

Strategy in the context of strategic cybersecurity management is about organisations ability to defend itself against offensive cyberattacks. You can't win the cyber war just by using defensive cybersecurity measures, but you can draw a line where offensive and defensive capabilities form a balanced state. Place where you are not vulnerable to an attack, but you are able to encounter and defend your organisations IT systems against to even the most sophisticated forms of cyberattacks successfully and stand your ground.

## References

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & security, vol. 86*, 402-418. https://doi.org/10.1016/j.cose.2019.07.001

Allen, M., & Cervo, D. (2015). *Multi-domain master data management*. Morgan Kaufmann. https://doi.org/10.1016/C2013-0-18938-6

Apple. (2022, April 24). *Privacy*. Apple. https://www.apple.com/privacy/

Australian Cyber Security Centre. (2022). *ACSC annual cyber threat report - 1 July 2020 to 30 June 2021*. Australian Government, Australian Signals Directorate. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

BBC. (2019, July 8). British airways faces record £183m fine for data breach. *BBC News*. https://www.bbc.com/news/business-48905907

Boehm, J., Dias, D., Lewis, C., Li, K., & Wallance, D. (2022, March 10). *Cybersecurity trends: looking over the horizon*. McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity-trends-looking-over-the-horizon

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information and computer security, vol. 23*(3), 317-332. https://doi.org/10.1108/ICS-09-2014-0064

Calder, A. (2013). *ISO27001/ISO27002: a pocket guide*. IT Governance Ltd. ISBN: 9781849285230.

Cambridge Dictionary. (n.d.). Meaning of cybersecurity in English. In *Cambridge dictionary*. Retrieved April 11, 2022, from https://dictionary.cambridge.org/dictionary/english/cybersecurity

Cambridge Dictionary. (n.d.). Meaning of governance in English. In *Cambridge dictionary*. Retrieved April 25, 2022, from https://dictionary.cambridge.org/dictionary/english/governance

Cambridge Dictionary. (n.d.). Meaning of management in English. In *Cambridge dictionary*. Retrieved April 13, 2022, from https://dictionary.cambridge.org/dictionary/english/management

Cambridge Dictionary. (n.d.). Meaning of strategy in English. In *Cambridge dictionary.* Retrieved April 11, 2022, from https://dictionary.cambridge.org/dictionary/english/strategy

Carvalho, J. V., Carvalho, S., & Rocha, A. (2020, January 22). European strategy and legislation for cybersecurity: implications for Portugal. *Cluster computing 2020-01-22, vol. 23*(3), 1845-1854. https://doi.org/10.1007/s10586-020-03052-y

CBS Boston. (2020, June 15). *6 eBay executives and employees charged with threatening natick couple* [Video]. YouTube. https://www.youtube.com/watch?v=NacqQW-SC7I

Center for Internet Security. (2022). *The 18 CIS Critical Security Controls*. Center for Internet Security. https://www.cisecurity.org/controls/cis-controls-list

Chatterjee, D. (2019). Should executives go to jail over cybersecurity breaches? *Journal of organizational computing and electronic commerce, vol. 29*(1), 1-3. https://doi.org/10.1080/10919392.2019.1568713

Cieslak, N. (2016, March 29). NIST cybersecurity framework adoption on the rise. *Tenable, Inc*. https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise

CISCO. (n.d.). What is cybersecurity? In *Cisco.com*. Retrieved April 11, 2022, from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cybersecurity & Infrastructure Security Agency. (2022). *2021 trends show increased globalized threat of ransomware* (AA22-040A*).* U.S. Department of Homeland Security. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

Cybersecurity & Infrastructure Security Agency. (2019, May 6). *Security tip* (ST04-001). U.S. Department of Homeland Security. https://www.cisa.gov/uscert/ncas/tips/ST04-001

Data Protection Commission. (2021, September 2). *Data protection commission announces decision in WhatsApp inquiry*. The Data Protection Commission

(DPC). https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

Defence Ministry of Finland [@DefenceFinland]. (2022, April 8). Puolustusministeriön verkkosivut defmin.fi ovat tällä hetkellä palvelunestohyökkäyksen kohteena [Tweet]. Twitter. https://twitter.com/DefenceFinland/status/1512365938217205760

Dimensional Research. (2016, March). *Trends in security framework adoption - a survey of it and security professionals*. Tenable. https://www.tenable.com/whitepapers/trends-in-security-framework-adoption

Doffman, Z. (2021, March 16). *No, Your iPhone is Not More Secure Than Android, Warns Cyber Billionaire*. Forbes. https://www.forbes.com/sites/zakdoffman/2021/03/16/iphone-12-pro-max-and-iphone-13-not-more-secure-than-google-and-samsung-android-warns-cyber-billionaire

Dog, S. E., Tweed, A., Rouse, L., Chu, B., Qi, D., Hu, Y., Yang, J., & Al-Shaer, E. (2016). Strategic cyber threat intelligence sharing: a case study of IDS logs. *2016 25th International Conference of Computer Communication and Networks (ICCCN)*, 2016, 1-6. https://doi.org/10.1109/ICCCCN.2016.7568578

Dutton, W. H., Creese, S., Esteve-González, P., Goldsmith, M., & Harris, C. W. (2022, February 15). Next steps for the EU: building on the Paris call and EU cybersecurity strategy. *University of Oxford, Oxford Martin School, Global Cyber Security Capacity Centre*. https://dx.doi.org/10.2139/ssrn.4052728

European Commission. (2017, September 13). *President Jean-Claude Juncker's state of the union address 2017*. European Parliament, European Commission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

European Parliament. (2022, January 27). *Cybersecurity: main and emerging threats in 2021 (infographic)*. The President of the European Parliament. https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic

European Union Agency for Cybersecurity. (2022). *National capabilities assessment framework (NCAF) tool*. ENISA. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/

European Union Agency for Cybersecurity. (2020, December). *National capabilities assessment framework*. ENISA. https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework/@@download/fullReport

European Union Agency for Network and Information Security. (2016, July 1). *Definition of Cybersecurity - Gaps and overlaps in standardisation*. ENISA. https://doi.org/10.2824/4069

Freedman, L. (2013). *Strategy: A history*. Oxford University Press, Incorporated.

Fortune. (2022). Fortune 500 - eBay. *Fortune Media IP Limited*. Retrieved April 29, 2022, from https://fortune.com/company/ebay/fortune500/

Galinec, D., Moznik, D., & Guberina, B. (2018). Cybersecurity and cyberdefence: national level strategic approach. *Automatika - journal for control, measurement, electronics, computing and communications, vol 58*(3). 273-286. https://doi.org/10.1080/00051144.2017.1407022

Gurijala, B. (2021, August 9). What is pegasus? how surveillance spyware invades phones. *Scientific American*. https://www.scientificamerican.com/article/what-is-pegasus-how-surveillance-spyware-invades-phones/

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of intellectual capital, vol. 21*(2), 203-213. https://doi.org/10.1108/JIC-05-2019-0112

Hepfer, M., & Powell, T., C. (2020). Make cybersecurity a strategic asset. *MIT Sloan Management Review, 62*(1), 40-45. https://www.proquest.com/scholarly-journals/make-cybersecurity-strategic-asset/docview/2450655586/se-2?accountid=14797

Horwath, R. (2006). The origin of strategy. *Strategic Thinking Institute*. https://www.strategyskills.com/Articles/Documents/origin_strategy.pdf

IBM. (n.d.). What is cybersecurity? In *Ibm.com*. Retrieved April 11, 2022, from https://www.ibm.com/topics/cybersecurity

IDG. (2020, March 31). The state of IT modernization 2020. *International Data Group*. Retrieved April 28, 2022, from https://www.insight.com/en_US/content-and-resources/2020/the-state-of-it-modernization-2020.html

Irwin, L. (2022, January 26). UK organisations have experienced a 62% increase in cyber threats since 2020. *IT Governance Blog*. https://www.itgovernance.co.uk/blog/uk-organisations-have-experienced-a-62-increase-in-cyber-threats-since-2020

IT Governance. (n.d.). Cyber security definition. In *itgovernance.com*. Retrieved April 11, 2022, from https://www.itgovernance.co.uk/what-is-cybersecurity

Jacuch, A. (2021). Comparative analysis of cybersecurity strategies. European union strategy and policies. Polish and selected countries strategies. *Online journal modelling the new Europe* 2021-12-22 (37), 102-120. https://doi.org/10.24193/OJMNE.2021.37.06

Jakkal, V. (2022, January 25). *How CISOs are preparing to tackle 2022*. Microsoft. https://www.microsoft.com/security/blog/2022/01/25/how-cisos-are-preparing-to-tackle-2022/

Johnson, J. (2021, November 15). Average cost per data breach in the United States 2006-2020. *Statista*. https://www.statista.com/statistics/273575/average-organizational-cost-incurred-by-a-data-breach/

Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *The Journal of business strategy, vol. 43*(1), 28-26. https://doi.org/10.1108/JBS-06-2020-0116

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organisations. *EDPACS, vol. 63*(6), 1-22. https://doi.org/10.1080/07366981.2020.1815354

Mandiant. (2022). Advanced persistent threats (APTs). *Mandiant*. Retrieved April 28, 2022, from https://www.mandiant.com/resources/apt-groups

Mehta, C., & Chee, F. Y. (2021, July 30). Amazon hit with record EU data privacy fine. *Reuters*. https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/

Merriam-Webster. (n.d.). Cybersecurity. In *Merriam-Webster.com dictionary*. Retrieved April 11, 2022, from https://www.merriam-webster.com/dictionary/cybersecurity

Merriam-Webster. (n.d.). Governance. In *Merriam-Webster.com dictionary*. Retrieved April 25, 2022, from https://www.merriam-webster.com/dictionary/governance

Merriam-Webster. (n.d.). Management. In *Merriam-Webster.com dictionary*. Retrieved April 13, 2022, from https://www.merriam-webster.com/dictionary/management

Merriam-Webster. (n.d.). Strategy. In *Merriam-Webster.com dictionary*. Retrieved April 11, 2022, from https://www.merriam-webster.com/dictionary/strategy

Mori, S., & Goto, A. (2018, July 11). Reviewing national cybersecurity strategies. *Journal of disaster research, vol. 13*(5), 957-966. https://doi.org/10.20965/jdr.2018.p0957

Nakashima, E., & Warrick, J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post*. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

National Cyber Security Centre. (2022). *Joint advisory highlights increased globalised treat of ransomware.* United Kingdom, National Cyber Security Centre (NCSC). https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

National Cyber Security Centre. (n.d.). What is cyber security? *In ncsc.gov.uk*. Retrieved April 11, 2022, from https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & management, vol. 58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507

Pang, M. S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: the case of U.S. federal government. *Journal of strategic information systems, vol. 31*(1), 1-19. https://doi.org/10.1016/j.jis.2022.101707

PCI Data Security Standards Council. (2022, March). *Payment card industry data security standard - requirements and testing procedures* [Version 4.0]. https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf

Perry, J. (2022, April 7). Is your small business ready for a cyberattack? survey say just half are. *Njbiz*. https://www.proquest.com/docview/2649443027

Pilke, A. (2022, January 28). Suomalaisia diplomaatteja vakoiltu haittaohjelmalla - ulkoministeriö: vakava tapaus, tulkitsemme laittomaksi tiedusteluksi. *YLE*. https://yle.fi/uutiset/3-12292218

Pohjanpalo, K. (2021, November 31). Finland battles 'exceptional' malware attack spread by phones. *Bloomberg Technology*. https://www.bloomberg.com/news/articles/2021-11-30/finland-battles-exceptional-malware-attack-spread-by-phones

Porter, M. (1985). *Competitive advantage: creating and sustaining superior performance*. Free Press; Collier.

Porter, M. (1996). What is strategy? *Harvard Business Review 74*(6), 61-78.

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, & Dwidevi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organization strategic cybersecurity management. *Technological forecasting & social change, vol. 170*(2021), 120872. https://doi.org/10.1016/j.techfore.2021.120872

Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity: building a successful defence program. *Front health serv manage, vol. 35*(1), 13-22. https://doi.org/10.1097/HAP.0000000000000037

Richter, F. (2022, February 8). Amazon leads $180-billion cloud market. *Statista*. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Rieder, F. (2022). *Advanced persistent threat - latest developments, potential impact and recommendations*. Deloitte. Retrieved April 28, 2022, from https://www2.deloitte.com/ch/en/pages/risk/articles/advanced-persistent-threat.html

Rudden, J. (2022, January 7). Cyber insurance - statistics & facts. *Statista*. https://www.statista.com/topics/2445/cyber-insurance/#dossierKeyfigures

Sharma, A. (2019). 5 ways cybersecurity awareness trainings can strengthen your organisation. *CIO*. Retrieved from https://www.proquest.com/docview/2312686701

Statista. (2022). Average organizational cost to a business in the United States after a data breach from 2006 to 2020. In *Statista.com*. Retrieved April 26, 2022, from https://www.statista.com/statistics/273575/average-organizational-cost-incurred-by-a-data-breach/

Taylor, A. (2022, February 17). There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps. *Fortune Magazine*. https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/

The General Data Protection Regulation. (2016). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

UK Government. (2021, March 24). *Cyber security breaches survey 2021*. Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

U.S. Attorney's Office. (2022, April 25). *Former eBay executive pleads guilty to his role in cyberstalking campaign*. U.S. Department of Justice, U.S. Attorney's Office,

District of Massachusetts. https://www.justice.gov/usao-ma/pr/former-ebay-executive-pleads-guilty-his-role-cyberstalking-campaign

US National Institute of Standards and Technology. (2022). *NIST Cybersecurity Framework*. U.S. Department of Commerce. https://www.nist.gov/cyberframework/framework

US National Institute of Standards and Technology. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Verizon. (2021). 2021 data investigations breach report. In *Verizon.com*, Retrieved April 30, 2022, from https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of applied security research, vol. 16*(4), 490-513. https://doi.org/10.1080/19361610.2021.1918995

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: cyberinsurance, managed security services, and risk pooling arrangements. *Journal of management information systems, vol. 30*(1), 123-152. https://doi.org/10.2753/MIS0742-1222300104

Zuopeng (Justin) Zhang, Wu, H., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: A cost-benefit analysis framework. *Industrial Management & Data Systems, 121*(3), 613-636. https://doi.org/10.1108/IMDS-08-2020-0462

# Appendices

## **Appendix 1.** Top 10 Origins of Cyberattack Events by Organisation

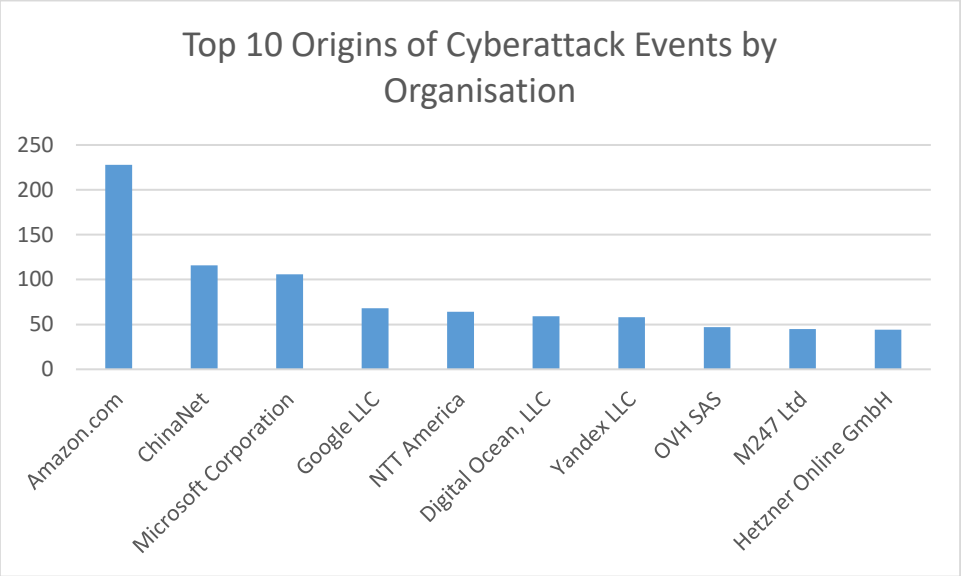


**Figure 14.** Top 10 origins of cyberattack events by organization.

Above appendix 1 shows recorded top 10 origins of cyberattack events by organisation to www.janipaivarinta.com. Data has been collected in the period of 2019/06/01-2022/04/11.

**Appendix 2.** Top 10 Origins of Cyberattack Events by Country

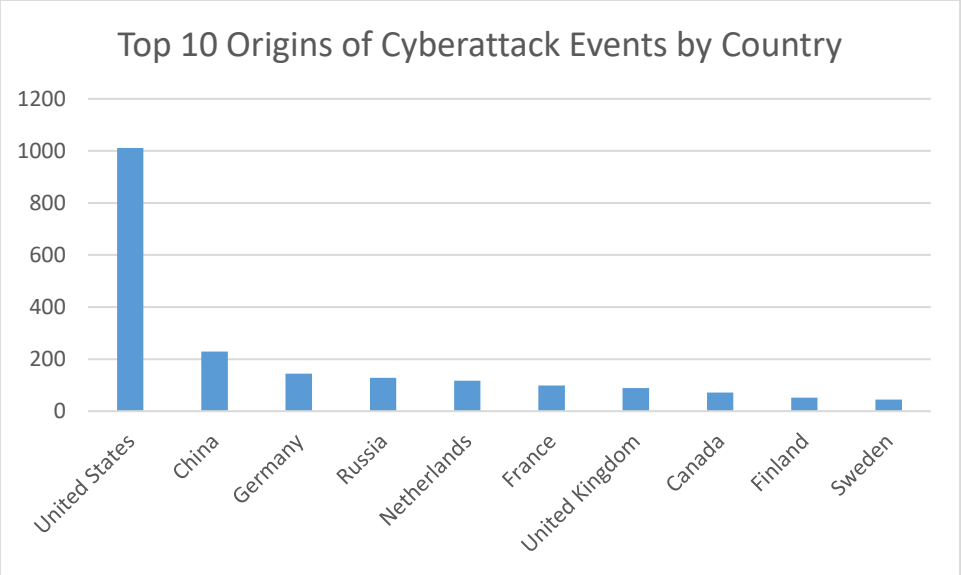


**Figure 15.** Top 10 origins of cyberattack events by country.

Above appendix 2 shows recorded top 10 origins of cyberattack event by country to www.janipaivarinta.com. Data has been collected in the period of 2019/06/01-2022/04/11.

**Appendix 3.** Top 10 Origins of Cyberattack Events by Platform

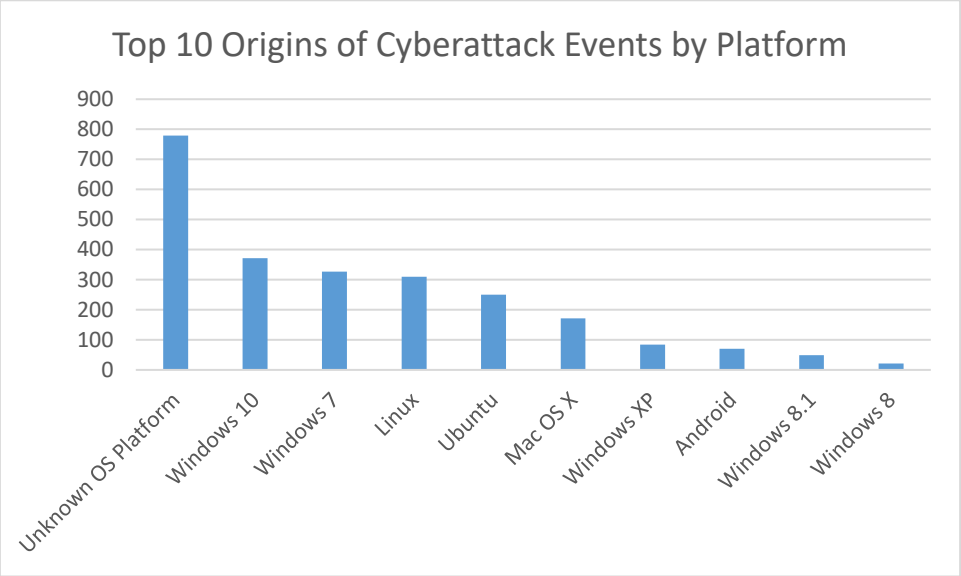


**Figure 16.** Top 10 origins of cyberattack events by platform.

Above appendix 3 shows recorded top 10 origins of cyberattack event by platform to www.janipaivarinta.com. Data has been collected in the period of 2019/06/01-2022/04/11.

**Appendix 4.** Top 10 Origins of Cyberattack Events by Browser

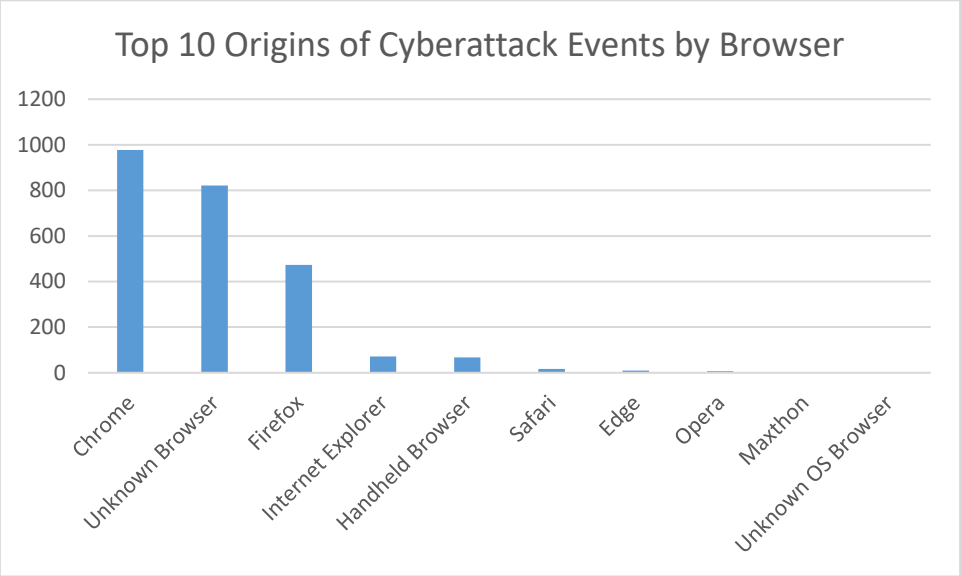


**Figure 17.** Top 10 origins of cyberattack events by browser.

Above appendix 4 shows recorded top 10 origins of cyberattack event by browser to www.janipaivarinta.com. Data has been collected in the period of 2019/06/01-2022/04/11.

**Appendix 5.** Top 10 Origins of Cyberattack Events by Region

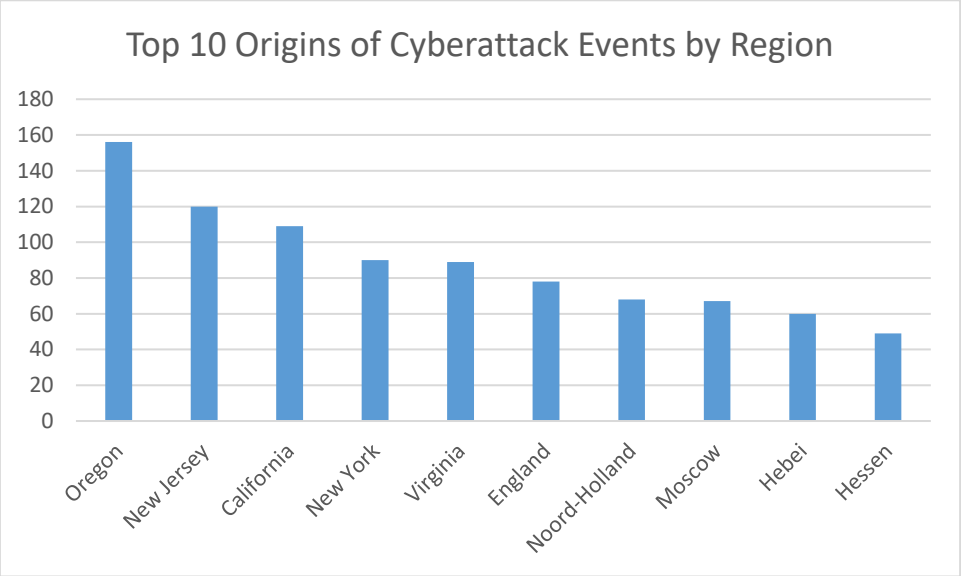


**Figure 18.** Top 10 origins of cyberattacks events by region.

Above appendix 5 shows recorded top 10 origins of cyberattack event by region to www.janipaivarinta.com. Data has been collected in the period of 2019/06/01-2022/04/11.