

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology

Department of Software Science

Fernando Garcia-Granados IVCM165633

**CYBERSECURITY KNOWLEDGE  
REQUIREMENTS FOR NON-IT STRATEGIC  
LEVEL DECISION MAKERS**

Master Thesis

ITC70LT

Hayretdin Bahsi

Tallinn 2018

## **Author's declaration of originality**

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Fernando Garcia-Granados

[07.05.18]

## **Abstract**

Recent surveys done in the field of cyber security have consistently shown that non-IT senior leaders are becoming and ever greater vulnerability to organizations. In order to lessen the vulnerability posed by senior leaders, they must be properly informed, trained, and provided with the necessary tools to make decisions to secure the organization's systems and assets. To begin the process of informing senior leaders, this study aims to provide a list of topics that would serve as knowledge requirements to be used as a basis for training or cyber exercises. An initial literature review of existing publications was done to select topics as well as further research was further performed into each topic. These selections were then derived into a set of 43 topics which were included as cards in a card sorting survey given to 10 professionals in the roles of CTO, CIO or CISO. The professionals were required to group the topics into four different categories denoting the level of knowledge non-it senior leaders should have on each topic. The results indicate that survey participants believe senior leaders should have a at least a general understanding and awareness of the topics chosen, even if the topics represent a more technical perspective, while also indicating the senior leaders should have knowledge of how the less technical topics are applied in their organizations. It was found that topics relating to business impact were ranked as requiring more knowledge from non-IT senior leaders. The study was limited due to the number of participants and all sharing the same role in an organization. Future studies can use the survey topics and results to develop training schemes or prepare for cyber exercises.

## Annotatsioon

Hiljutistest küberkaitse uuringutest on välja tulnud, et mitte-IT haridusega kõrgastme juhid muutuvad järjest suuremaks küberohuks organisatsioonidele. Kõrgastme juhte tuleb õigesti koolitada, informeerida ja neile tuleb võimaldada õigeid tööriistu otsuste tegemiseks, et vähendada nende poolt tekitatud tahtmatut ohtu organisatsiooni varale ja süsteemidele. Antud uuring pakub välja erinevad teemad, mida kõrgastme juhid teadma peaksid ning mis paneb aluse erinevatele küberkaitse õppeharjutustele organisatsiooni siseselt. Kõigepealt tehti esialgne kirjanduse ülevaade, et välja valida teemad, mis antud lõputöös välja pakutakse ning peale seda uuriti igat teemat individuaalselt. Nendest valikutest tuletati välja 43 teemat, mis muudeti kaartideks, neid kaarte kasutati uuringus, kus kaardid anti kümnele eriala professionaalile (CTOd, CIOd või CISOd). Küsitluses osalenud professionaalid pidid kaardid grupeerima nelja erinevasse kategooriasse, tuginedes sellele kui palju kõrgastme juht peaks igat teemat valdama. Tulemused näitasid, et uuringus osalenud uskusid, et kõrgastme juhid peaksid omama üldistaruusaama ning olema teadlikud antud teemadel, isegi kui teemad esindavad rohkem tehnilisi aspekte. Uuringust tuli ka välja, et kõrgastme juhid peaksid teadma ka vähem tehnilisi küberkaitse aspekte ning kuidas need nende organisatsiooni mõjutavad. Uuringus leiti ka, et teemad, mis võivad ärile mõju avaldada peaksid olema kõige selgemad. Antud uuringu piiranguks oli fakt, et uuringus osalejate arv oli väike ning nad jagasid kõik sama rolli oma organisatsioonis. Tulevastest uuringutes saab selle uuringu tulemusi ja teemasid rakendada, et luua koolitusi ning ettevalmistavaid materjale küberõppusteks.

## **Table of abbreviations and terms**

SLDM	Strategic level decision maker
IS	Information Security
KSA	Knowledge, skills, and abilities
BoK	Body of Knowledge
KE	Knowledge elicitation
APT	Advanced Persistent Threat
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CTO	Chief Technology Officer

# Table of Contents

1. Introduction .....	9
1.1. Problem statement.....	9
1.2. Motivation.....	10
1.3 Related Works .....	11
2. Research Design .....	14
2.1 Desk Review.....	14
2.3 Survey development .....	18
2.3.1 Survey methodology.....	18
2.3.2 Survey participant selection.....	20
2.3.3 Survey analysis .....	21
3. Desk Review.....	23
3.1 Raw Matrix Results .....	23
3.2 Incidence Percentage .....	25
4. Topic Description .....	29
5. Survey Elaboration .....	46
5.1 Survey Tool .....	46
5.2 Card List .....	50
6. Results .....	54
6.1 Raw Results.....	54
6.2 Best Merge Method .....	56
7. Summary.....	62
8. Conclusions and Future Research .....	67
Appendix 1 – Sources for Desk Review.....	76

## **List of figures**

Figure 1. Literature Research Results Matrix.....	27
Figure 2. Literature Research Results Ranked .....	28
Figure 3. Welcome Screen.....	46
Figure 4. Instructions.....	47
Figure 5. Survey Example .....	49
Figure 6. Survey End.....	49

List of figures enlists only figures presented in the main part of the thesis, figures in appendixes are excluded.

## List of tables

Table 1. Survey Participant Industry and Org. Size .....	21
Table 2. Card List .....	52
Table 3 Raw Survey Results.....	55
Table 4 Best Merge Display .....	58
Table 5 Summary of Results .....	62

List of tables enlists only tables presented in the main part of the thesis; tables in appendixes are excluded.



# **1. Introduction**

The topic of the thesis is “cyber security knowledge requirements for non-it strategic level decision makers” with the aim of deriving a list of concepts in the realm of cyber security along with a recommend level of knowledge that strategic level decision makers should have on the topic.

## **1.1. Problem statement**

Cybersecurity has been a trending topic in recent years with cybercrimes seemingly becoming more and more commonplace, in fact, it is predicted that by 2021 the cost of cybercrimes will reach about 6 trillion USD per year worldwide [1]. With the advent of rising cybercrimes, it is now of the utmost importance for private organizations to be prepared for the eventuality of a cyber-attack. In recent studies, it has been found that CEOs and other C-level executives pose the greatest threat to an organization from a cyber security standpoint [2]. C-level’s high position within the organization means an attack against them has the potential to be more disruptive, as such it’s important to mitigate the threat C-level executives pose to the organization through proper training and educating these executives in how to best protect the organization.

Part of the problem lies with CEOs and other C-level executives not having proper security training to properly oversee the avoidance and mitigation of threats as well as not having adequate knowledge to make decisions that affect the way an organization will protect its data and systems from cyber threats. In a survey done in 2015[3], it was found that 43% of management teams were not briefed on cyber incidents and security issues; there is a lack of communication between upper management and the information security branch of organizations. Given that upper management makes decisions that affect the way an organization handles its security operations, it is important for upper management to have a clear, defined understanding of how the organization aims to protect its assets from cyber threats as well as there being open channels of communication between upper management and the organization’s cyber defense teams. In order for the organization’s strategic level decision makers (SLDMs) to have this defined understanding, different topics in the realm of cyber security need to be defined in order for these decision makers to begin the learning process.

Upper management's engagement with risk oversight is becoming more involved [4]. As upper management becomes more involved with an organization's security processes, there is an even greater need for upper management to be better educated in the realm of cyber security so that they may make more informed decisions.

## **1.2. Motivation**

Many modern-day cybersecurity certifications or training are specially fitted to finding a technical solution to what is perceived as a technical problem [6]. As such, these advanced certifications focus on defining competencies for technical professionals while largely ignoring the potential to educate non-technical professionals. Most importantly, it is often not these technical professionals who lead an organization, as such many organizations are being led by professionals with little knowledge in information security.

From the former National Security Council Director for Cyberspace in the USA: "If you are the CEO of a major corporation, you need to understand the contribution of ICT to the bottom line and how it affects your efficiency and productivity, but you also need to understand when the policies and programs in place are affecting your risks if you have a security breach." [6]

The role non-IT SLDMs have in an organization's security operations is becoming more and more prevalent. As such, these decision makers need to have a basis of understanding of different concepts so they can make better decisions.

The motivation behind this thesis study is to begin the process of solving the problem of how to adequately educate non-IT SLDMs in matters of cybersecurity. In order to properly educate senior executives, a set of knowledge, skills, and abilities (KSA) are required. This thesis will focus on determining the set of knowledge requirements through a review of the current literature to compose a list of terms and topics which will then be presented in survey form to a selection of CISOs, CIOs, and CTOs with the purpose to rank what level of knowledge non-IT SLDMs should ideally have on each of the topics and terms. The list could in the future be used to derive skills and abilities related to each term of knowledge as well as being used to develop training programs with the specific focuses in mind. The list could also serve as a starting point for senior managers to begin their own education into cybersecurity as well as motivate them to start doing so.

### 1.3 Related Works

An AT&T report [7] on “What every CEO needs to know about cybersecurity” covers some basic topics but no in-depth review is provided and mainly focuses on biggest threats organization’s currently face. A simple guide is also provided “The CEO’s guide to navigating the threat landscape” [8] in which some terms such as malware, ransomware and concepts such internet of things and risk and vulnerabilities are explain. Both of these studies focus on definitions and lack a wider array of topics in the field of cyber security.

Different certification agencies have derived their own knowledge requirements for professionals working in technical fields such as cybersecurity [9][10][11]. Certifications like CISSP define a common body of knowledge from which the professional must have knowledge of. This body of knowledge serves as a knowledge requirement but its specifically targeted at IT and cyber security professionals requiring to pass an examination and years of experience in the field.

The certification for governance of enterprise IT(CGEIT) [12] defines knowledge statements in the topics of IT governance, strategic management, benefits realization, risk optimization, and resource optimization. This certification is meant for professionals with more than five years in an IT governance position which would disqualify many non-IT senior level managers as they would lack that distinction. This certification proposes many in-depth knowledge requirements in the topic of governance but its aimed at IT professionals. Similarly, the (ISC)2 defines their own body of knowledge and include topic that serve as knowledge requirements [13] but their focus is on technical professionals.

The book “Cybersecurity: The Essential Body of Knowledge” defines competencies to the role of “the Boss” [14]. These cover a variety of topics from incident handling, business continuity, to regulatory compliance. The book focuses on explaining the CIO in the role of the boss and not other non-IT upper management positions in this role. The book also approaches the subject from a role and competency point and not of defining requirements and levels of knowledge associated with them.

There have been several publications that discuss the role of different non-IT upper managers have in the topic of cybersecurity [15][16][17][18][19]. These publications define different roles that CFOs, CEOs and other C-Suite executives have in their

organization's cyber security operations. Different competencies were mentioned but no in-depth study is shown and are mostly focused on one role within the organization.

UCISA defines roles and competencies in their Information Security Management Toolkit [20]. This toolkit defines a small number of roles for top managements or decision makers. They cover information security strategy and governance. The competencies named for top management are few.

A report [21] published by the Pell Center for international relations and public policy describes the need to create a common KSA for information security professionals as well as the difficulties in determining what to include and who would regulate it. The report also discusses how these KSAs might apply to non-IT managers and how it is essential for them to be included in being educated in the field.

An article [22] published by MIT Sloan Review discusses the issue of educating company leadership and provides small insight into the kind of knowledge to be educated. The article mentions the topics of business continuity and disaster recovery as well as security controls, preventive measures, and security strategy.

The US Department of Homeland Security has prepared a document [23] concerning CEOs and cyber risks while defining a few key cyber risk managements concepts the CEO should be aware of.

There have been related studies into the derivation of knowledge requirements in other fields of study. For example, the University of Cambridge has derived knowledge requirements needed for researchers [24]. The requirements read more like core competencies and provide more of a sample rather than an in-depth guide.

A much older study [25] on the elaboration of knowledge requirements in the field of information security was published by the University of Michigan however this study focused on requirements for information security professionals instead of non-IT management. A public forum was first set up to gain a general understanding and then different surveys were created that targeted different groups: IS managers, business managers and IS consultants. The main focus of the study was to find what these groups thought was necessary knowledge for IS professionals in the IS security field.

A study [26] by the American Society for Clinical Pharmacology and Therapeutics aimed to derive competencies for professionals in the role of mentors of clinical and translation scholars. The methodology was to derive competencies from a literature search and present them to an expert panel. This methodology was similarly used in this thesis study.

A study by the University of Iceland aims to find knowledge requirements necessary for project managers to be proficient [27]. In this study, the researcher first derives 18 topics, ranging from resource management to cost legal issues, from previous research and then asks a panel of project management experts to place each of the 18 topics in such a way that each category is a slice and end up forming a circle with topics (leadership, strategy, execution, craftsmanship) on the four cardinal points. The results were then compared to the current research in journals and teachings in textbooks.

The current reports and surveys done on CISO do not focus on specific requirements which senior leaders should know, they mainly focus on recognizing senior leaders as vulnerabilities [2]. Other parts of the literature, such as the AT&T [7][8] reports, the USA government report [23] and the Pell Center report [21], do not provide the reasoning behind their recommendations and do not mention any scientific method used to reach said conclusions. Other areas of the literature provide recommendations of realms of knowledge but specifically target IT leaders [12][13][20]. The missing point is a report done using a scientific approach to specifically target knowledge requirements aimed at non-IT senior leaders and provide the proof behind the conclusions.

## **2. Research Design**

The main goal of the thesis is to derive a list of knowledge requirements, but in order to reach this goal a process of developing these requirements must be followed. The process was as follows:

1. Perform a desk review to derive a list of initial topics. Twenty different publications were used to develop a matrix to find the number of occurrences of topics.
2. Perform further research on each topic to determine of topics needed to be combined or further divided.
3. Use the research to develop cards for a card sort survey used to elicit knowledge from C-level IT positions.
4. Deliver card sort survey in electronic web-based form to 10 professionals in the role of CIO, CTO, or CISO.
5. Analyze results from survey using best merge method.
6. Present survey findings with incidence percent in table format

### **2.1 Desk Review**

The existing literature provides a starting point for deriving these requirements. As the first step in the research, I will look at what the existing literature is telling us. Since many pieces of the literature provide short analysis or analysis that cover few topics in the realm of what non-IT SLDMs should know, I chose to aggregate this research from which I will obtain an initial set of knowledge requirements which I can work with.

The first step is to choose articles from which I will be obtaining the information from. I decided to follow the following criteria for electing articles to be part of the study:

- Report or publication from a well-known organization
- Report or publication from a government organization
- Publication from an expert in the field of cyber security
- Peer reviewed study
- Documented standard from a regulatory or standards organization
- Body of knowledge from a certification organization
- Publication from organization in the field of cybersecurity

- Report or publication from a professional's association related to C-level executives

The principal idea is to obtain different viewpoints to compile the information. A large organization might have different viewpoints as to what is relevant for senior executives to know rather than what a government agency would like executives to know. While peer-reviewed studies would be ideal, I decided to include reports and publication from well-known organizations as it is these organizations that are dealing with senior executives who are lacking cybersecurity knowledge as well as their experience in dealing with the issue is also very valuable. I am also taking into account what experts in the field have to say about the issue as they are knowledgeable in the topic.

Standards organizations, such as (ISC)2 or ISACA, have composed their own bodies of knowledge which include roles and responsibilities. From these roles and responsibilities, it is possible to reverse engineer the required knowledge, which is why I chose to include these in the study. Several publications define what activities senior leaders should be engaging in with respect to the organization's cyber defense processes. For example, if a publication states that senior leaders should oversee or take active part in the organization's risk assessments, then it follows that senior leaders should have an idea or some knowledge in regard to risk assessment. The level of knowledge is not stated, it is information that would be vital when deciding what to include in a training program for example. Having minimal knowledge of risk assessment to having advanced knowledge is a great difference. On one end we could have knowledge of how to read a risk report and understand what information is presented. If minimal knowledge, the reader would not know how to create said document or how it relates to other processes and reports. If advanced knowledge, the reader would know how this document was created, what the process to assess risks is, and what are people's roles and responsibilities in a risk assessment.

Several publications developed their recommended roles and knowledge in the form of questions to ask senior leaders. From these questions, it is also possible to reverse engineer and derive what knowledge is being asked about and present that knowledge as a requirement, in other words, what knowledge requirements satisfies the question. For example, the question: How many cyber security policies are being actively managed? From this question it is possible to derive that senior leaders should have an understanding

of security policy management. Information presented in question forms also provides us with some insight into the proposed level knowledge to be had. In the example its asking about oversight of security policy, not the intimates of the security policy creation process

Documented standards refer to standards organizations such as ISO or NIST which also develop their own defined domains. For example, ISO27001 has 11 defined domains [28] ranging from security policy, organization of information security, to incident handling and compliance. While these standards and domains are not directly meant for non-IT senior leaders, these organizations have subdivided the field of cyber security for organizations in such a way we can turn the domains into topics and use them, in conjunction with other sources, to create the topics to be presented in the survey. ISO also provides us with objectives, which like roles, can also be reverse-engineered to derive a knowledge requirement.

Professional executive organizations like the International Federation of Accountants (IFAC) provide us with a perspective from a non-technical viewpoint into what executives in that role should know in cybersecurity. While not being IT technical professionals, these kinds of organizations provide us with insights into what different non-IT roles like chief financial officers (CFAs) believe what others in their positions should have knowledge of. Having the viewpoint from an organization representing professionals we are creating the requirements for lets us leverage what IT professionals might consider something that non-IT senior leaders should know but these senior leaders might believe is out of the scope of their roles.

## **2.2 Topic derivation**

After the literature research of the 20 publications is completed, the information needs to be aggregated and presented in such a way that repeating topics are found. The way this information was chosen to be derived was to create a matrix of incident recurrences on topics in each publication. The X axis of the matrix was filled with the publications, numbering at 20 total, while the Y axis was filled with the topics extracted from the publications. If a new topic was found, then a new row was added. If the topic was found in a publication, then the corresponding XY cell was marked as so.

Presenting data in this way lets us quickly analyze the times of occurrence a certain topic appears in the literature. This is also a simple way to keep adding topics as rows while



first revising if the topic already exists. When going over a publication, one only needs to focus on the specific column and the already existing rows. At the moment of data insert, one does not need to refer to previous publications as the relevant information was already included as a row in the matrix.

Topics can be displayed by order of incidence thus displaying which ones are the most popular in the literature. This incidence information combined with the survey results can give us an idea of what topics are important for non-IT senior leaders to have knowledge of and which topics are less relevant. All topics on the matrix were included however they are also noted for having a low incidence rate in the literature. They were included as the number of topics was not overwhelming thus needing to only include the most relevant topics but also as some of the publications might have different views on what should be relevant knowledge and thus including the lower incidences helps to create a wider view on the topic.

After the matrix was complete, a document, dubbed topic descriptions, was compiled with each of the topics further explaining what each topic means and in short, the relevance it has to senior leadership. This document aims to briefly explain the topics to readers and was also used to explain what the topics mean to participants in the survey. Each topic is presented in one to three sentences of what the topic is followed by a brief description of the topic explaining what the topic is composed of, the steps of a process, or the meaning behind an acronym. There is also brief explanation of why the topic is relevant to senior leaders as was described in the literature research publications.

The topic descriptions document was used to add additional information topics in the survey as well as further breaking down the topics presented in the publications. The publications might make reference to a certain topic, but upon further inspection in the descriptions document, that topic could be further broken down into two or more topics to make the survey clearer and provide us with more specific information. The descriptions are not meant as in-depth reviews on each topic but merely used to explain what the topic as well as describing its main components, if applicable.

## **2.3 Survey development**

This section shall discuss the survey that was sent including what kind of survey methodology was used, why that methodology was chosen, what was the criteria for selecting participants, and how the results of the survey will be presented. The methodology of using a survey was chosen for this study as it presents us with the views of professionals and senior leaders in the field of cybersecurity who deal with non-IT senior leaders.

### **2.3.1 Survey methodology**

The methodology chosen for the survey was to use the Card Sorting method. The card sorting method involves giving the participant a number of cards and asking them to sort the cards into groups [29]. The grouping can be pre-created by the survey creators, known as closed sorting, or the grouping can be left to the respondents, known as open sorting. It is generally used to survey small subsets of a given population due to the number of cards involved and purposive selection of respondents. Card sorting is used to derive a participant's attitude, feelings, or behavior as the participant relates to the topic of the study [30].

Card sorting can be used so participants can assign a pre-specified rank to a specific card. The categories can be pre-defined and displayed in an order that makes sense for the participants as in increasing magnitudes. For example, participants might be asked to sort cards with activities in them and the categories presented are different levels of proficiency, participants would then group activities into the category they believe corresponds with the level difficulty related to the activity. For example, an activity might be "flying an airplane" and categories could be: novice, experienced, expert.

Traditional card sorting is done using paper cards and asking participants to group them. The delivery method is done physically in-person face to face with the participants. Modern web technology has opened up the possibility of performing card-sorting activities over web tools. While the web method leaves out the possibility of recording the decision-making process of the participant and what they're willing to share, it also opens up the possibility of further reach as the need to be physically present presents a great limitation in reaching participants. However, the final product of the two types of

delivery method would be the same, different groups with cards corresponding to them and as such we can analyze the information similarly.

Card sorting was chosen for this study as it is effective and quick in eliciting domain knowledge from experts and knowledge of domain structure [30]. The main purpose of the study is to find knowledge requirements and their associated knowledge levels for non-IT senior managers. Since the survey includes IT specific SLDMs, such as CISO, CTO, and CIO roles, they can be considered domain experts in the field of cybersecurity and as such their knowledge into what should be known by non-IT senior staff is valuable. Closed card sorting was chosen as the study already had the pre-defined categories. In essence the study is attempting to find a level of knowledge so the categories can be defined into four: none, minimal, moderate, advanced. None means senior leaders have no need for knowledge in this topic. Minimal means senior leaders only need to have general awareness and know of the topic's definition. Moderate means senior leaders need to know how a topic is used or of its composition. Advanced knowledge means senior leaders should know how to use the topic, if applicable, and what roles and responsibilities are associated with said topic. Since the study tries to define each topic into those four categories, a closed card sort was used with the previous four denominations as categories. Web based card sorting was chosen for the easier reach to participants.

Other survey methodologies were considered. Laddering was discarded as its main purpose is to elicit goals [32] and not knowledge. A traditional survey where respondents are asked to choose an option from multiple choice was also considered but it was considered to be too cumbersome for participants to do so for more than 40 topics. It also lacked the impact of being able to see how a group is composed which is one of the features of a card sort exercise. A structured interview approach was also considered but ultimately discarded due to limitation in access to the participants. Another issue with a structured interview is the breadth of the topic, if participants were asked to describe what they thought senior leadership should know in terms of cybersecurity, the answers could be too varied to draw meaningful data. Even with pre-defined topics, the experts would be asked if the topic was something senior leaders should know and to what level. It would be better organized in a card sort form. While the meaningful commentary is lost

by doing it through a web form, the limitations outweigh the meaningful commentary in this study.

### **2.3.2 Survey participant selection**

For the purposes of this study, it is required that participants are suited to the following guidelines:

1. Be a strategic level decision maker in an information security or information technology senior role
2. Be part of an organization with 10 or more employees
3. Be in the United States

The roles that would fit the first requirements are chief information security officer, chief information officer, and chief technology officer. However, not all organizations use this specific nomenclature which is why the requirement does not mention specific named roles. It is also expected that these professionals have a large understanding and knowledge in the topic of cybersecurity. Since the study requires the view from security professionals on senior management, it was decided that only strategic level security positions would be used as it is professionals in these positions would be mostly dealing with other non-IT SLDMs

The second requirement was chosen as to target organizations larger than micro. The European Union defines an organization being micro as having less than 10 employees [33]. Smaller or micro organizations might not have the sufficient staff to have a full-time information security role. Smaller organizations might also lack any significant number of senior leaders thus meaning that security professionals in these organizations would lack much interaction with non-IT senior leaders meaning their input would be less valuable.

The third requirement was chosen because the survey language is in English as well as the ease of access to participants in the USA as well as the author being from the USA.

The methodology to choose participants was convenience sampling. The participant requirements mean that participants need to be in a highly advanced position in a technical field. The limited sample was due the difficulty in gaining access with participants in the

roles of CIO, CTO, or CISO, meaning that there is the downside of being vulnerable to selection bias and a low sample margin.

The participant's industry and organization size is presented in Table 1. All participants are part of organizations located in southern California, Florida, Connecticut, and the Greater Boston Area.

*Table 1. Survey Participant Industry and Org. Size*

<b>Participant Number</b>	<b>Industry</b>	<b>Organization Size</b>
1	Business Consulting	15
2	Healthcare IT Consulting	200
3	Marketing	20
4	Tourism and Travel	25
5	Industrial Engineering	50
6	Parking Services	500
7	Industrial Electronics	145
8	Full-service Marketing	50
9	Financial Services	60
10	IT Consulting	80

### **2.3.3 Survey analysis**

The survey results will first be displayed with the percentage of incidences recorded, in other words, how many times a card was chosen in each category. This would give an overview of the results and help begin to draw conclusions from the survey. From this view it would be clear if a specific card was overwhelming chosen in a specific category.

The cards would then be analyzed using the Best Merge Method [29]. The cards and categories will be placed in a matrix with the number of occurrences in the fields between them. The number of occurrences would then be replaced by percentage in each category. The cards would then be rearranged so that they're are grouped by highest occurrence percentage in group. This analysis would let us distinguish which cards fit most to each

category and from here we can draw conclusions as to which topic is more important as knowledge to senior leaders and which are not.

### **3. Desk Review**

This section shall cover the results of the literature section as well as provide analysis into the results that were obtained. The results will be first displayed in their raw matrix form and then each topic will be presented with a percentage of incidence and they will be ordered by their incidence rate.

#### **3.1 Raw Matrix Results**

Figure 1 presents the visualized results of the literature research done on 20 different publications. The decision to limit the research to 20 publications was reached as there is enough different kinds of publications included as well as few to none new topics being continually added. The main knowledge topics were obtained from each publication and presented on the matrix. The publications presented in the matrix are provided in Appendix 1.

The X axis on the matrix represents each of the publications listed as a number, from 1 to 20. The Y axis on the matrix represents the topics obtained from the publications. When a new topic was found, a new row was added. If there is an “x” present in the field combination (X,Y) then that means that specific topic was found in the corresponding publication.

Before analyzing the number of incidences, we can begin to draw conclusions based on the raw data. We can see the kinds of topics that are mentioned in the literature. We can see that the topic of Risk is continually referred on the literature, whether it be what is risk, risk management, and asset management including risks to most important assets. Of note was the idea that senior leaders should be aware of the organization’s highest risks. For this reason, the inclusion of what is a risk was added. Publications also mentioned that senior leader should know which are the organization’s most valuable assets, for this reason asset management was included.

Incident management was also included in the form of what constitutes an incident, how to manage incidents in the organization, and what is the process to elevate incidents. Incident management was also referred to as knowing what are the organization’s past incidents and how they were handled.

Given that the research looked for knowledge of senior leaders, there were several derived topics that deal with governance and strategic planning rather than tactical planning. Topics such as business continuity, security policy management/creation, cybersecurity committee, and cyber security planning involved decisions made by those in a higher level senior position and relate to how the organization handles security from a strategic level.

Insider threats were continually mentioned in the literature. Along with these threats there were recommendations of vetting employees and doing continual audits on employee records. Employee security management goes beyond insider threats and as such both topics were combined into the topic human resources security. This encompasses the mitigation of insider threats.

Threats were a topic that was frequently covered. It involved knowing what are the organization's top threats, as well as knowing of upcoming threats like internet of things threats. Publications also mentioned the existence of advanced persistent threats and how senior leaders should be aware of these more serious threats. Types of threats refers to knowledge on threats not being static and with many differences. Threats can be a malignant outsider or an employee unknowingly and non-maliciously damaging an organization's asset.

Business continuity was also frequently covered and refers to senior leaders being aware of how resilient and the organization's steps to recover from attacks. Business impact was chosen as a separate topic as publications referred to the cost, both in monetary terms and reputation that disruptions cause the organizations. Business continuity and disaster recovery were combined as they were mentioned in conjunction with each other in the publications.

Of note is the lack of technical aspects of cybersecurity. Cryptography was not mentioned and neither were any network security topics. Other than incident management, forensics topics were also not mentioned. However, access controls and secure software development were mentioned. Secure software development was mentioned in the context of senior leaders knowing the security status of a software project. Access controls were mentioned in the context of preventing or mitigating insider threats. Even



though there were few technical topics mentioned, risk mitigation strategies were mentioned even though no specific technical controls were defined.

### **3.2 Incidence Percentage**

After analyzing the results from the raw matrix (Figure 1), the topics were ranked in a table displaying the number of incidences in the literature and are shown in figure 2. The topics are sorted from highest percent of incidence at the top and the least at the bottom. The highest and lower ranked topics will be briefly discussed.

The most recurring topic is risk management followed by cybersecurity asset management. This mostly involves senior leaders knowing about the organization's most critical assets as well the risks related to those critical assets. We can deduce that the literature supports the idea of senior leaders knowing about risk and risks affecting their organization. Along with risk is the topic of business impact, impact is part of the definition of risk so that could be the reason why it was also ranked high.

Next, we can see that cyber incident management was ranked high at 50% but incident elevation is ranked at 30% and cyber incident response 25%. This can be interpreted as knowledge of how the incident process works or how incident information is reviewed is more valuable to senior leaders. Information about the process of how to report incidents or what is the criteria for an incident to be elevated is of less importance.

Cyber security policy creation and policy management have a similar number of incidences, 9 and 7 respectively. This can be interpreted as senior leadership needing to know how to properly set security policies for their organization as well as reviewing their effectiveness. Given that policy management mainly deals with governance it is reasonable to see it being repeated in the literature.

Industry standards was ranked with a 45% incidence rate. The literature recommended for senior leaders to be aware if their organizations are in compliance with standards or if their organizations are following any standards framework. However, the literature did not recommend for senior leaders to be familiar with the standards themselves, merely knowing of their existence and how well was the organization in complying were the recommendations.

The literature recommended for senior leaders to take an active part in overseeing their organization's security training programmers, as such we can see cybersecurity awareness and training with a 45% incidence rate.

The topics with the least number of incidences were topics mainly detailing more technical aspects of information security or topics outside the realm of governance. Secure software development was only mentioned once and it was with the recommendation of senior leaders being aware of the process to develop secure software so that they could effectively communicate with IT leaders as for the status of the project.

Access controls were also only mentioned once. It is mainly a technical topic dealing with how to securely access data. In the literature, it was recommended that senior leaders are aware of what kinds of access controls are in place, the same recommendation was present for application monitoring. The literature recommends that senior leaders are aware what kinds of tools the organization uses to monitor its applications. These low ranked topics mainly deal with senior leaders being aware of security operations in the organization.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Cybersecurity Asset Management	x	x	x	x		x	x	x	x	x			x			x	x			
Risk Management	x	x		x	x	x	x	x	x	x		x	x	x	x	x		x	x	x
Cybersecurity Policy Creation	x		x	x	x	x	x			x	x							x		
Cybersecurity Awareness and Training	x	x		x		x	x			x					x				x	x
Security Policy Management	x								x	x							x	x	x	x
Incident Elevation	x	x		x		x			x	x										
Human Resources Security		x	x	x		x							x							x
Reputation/Risk		x		x	x			x				x	x	x				x		
Cyber Incident Management	x	x					x	x	x		x				x		x	x		x
Industry Standards/Compliance		x	x	x			x		x		x	x		x		x				
Cyber Incident Response		x						x							x	x		x		
Cybersecurity Insurance		x						x	x											
Cybersecurity Plan/planning		x						x			x	x		x		x	x		x	x
Cybersecurity Committee	x	x		x				x			x	x		x	x					
Organizational Security	x	x	x	x		x				x	x									
Business Continuity/Disaster Recovery			x		x	x	x						x		x			x		x
APT				x																
Types of Threats/emerging risks				x		x		x			x		x			x				
Auditing Methods				x				x	x					x			x	x	x	
IoT Threats		x		x									x							
Supply Chain Security				x			x	x	x				x		x		x			
Application Monitoring																	x			
Layers of Security				x	x	x														
Secure Software Development														x						
Customer Relationship Management					x			x			x	x								
Manage Data Security							x													
Business Impact	x	x		x	x		x	x	x	x					x	x				x
Threat Mitigation													x	x	x		x		x	
Access Controls													x							

Figure 1. Literature Research Results Matrix

Topic	Incidences	Incident percent
Risk Management	17	85%
Cybersecurity Asset Management	12	60%
Business Impact	11	55%
Cyber Incident Management	10	50%
Cybersecurity Policy Creation	9	45%
Cybersecurity Awareness and Training	9	45%
Industry Standards/Compliance	9	45%
Cybersecurity Plan/planning	9	45%
Reputation/Risk	8	40%
Cybersecurity Committee	8	40%
Business Continuity	8	40%
Security Policy Management	7	35%
Organizational Security	7	35%
Auditing Methods	7	35%
Supply Chain Security	7	35%
Incident Elevation	6	30%
Human Resources Security	6	30%
Types of Threats/emerging risks	6	30%
Cybersec Comitee	6	30%
Cyber Incident Response	5	25%
Threat Mitigation	5	25%
Customer Relationship Management	4	20%
Cybersecurity Insurance	3	15%
IoT Threats	3	15%
Layers of Security	3	15%
APT	1	5%
Application Monitoring	1	5%
Manage Data Security	1	5%
Access Controls	1	5%
Secure Software Development	1	5%

*Figure 2. Literature Research Results Ranked*

## 4. Topic Description

Having attained a list of 30 topics from the literature, this section will use further brief research into each topic and present information about each topic. The purpose of this section is to decide if certain topics need to be split into more or if others need to be combined. The survey will include both the name of the topic in each card as well as a brief description of each topic which will be obtained from this section. Each topic will be briefly described in a single sentence with a small description following. The topic from the matrix shall be also included.

### **Full scope vs limited scope penetration testing – Auditing methods**

Having a penetration test with a well-defined scope due to data sensitivity or host requirements has the downside of the inability to test against unknown attackers and how to respond to a breach in the restricted sector. "It's now not a question of whether a business will be hacked but when"[35] By limiting access for testers decision makers are creating blind spots in their organization's network that are vulnerable to attack. While it may lead to a drop-in performance or the potential to create complications, a process of Calcification [36] is useful to properly perform full-scope penetration tests. Calcification means that an organization would continually prod and pen-test their production environment and other sensitive systems to continually harden them while knowing that it may cause issues with the idea of acting like an actual outside attacker would.

### **Penetration Testing Selection Process – Auditing methods**

There is a difference between vulnerability assessment and penetration testing. Vulnerability assessment uses widely available scanning tools to scan the organization. The upside is that its quick and easy to do and thus cheaper but it can only scan for vulnerabilities included in the tools, it is not complex and it's not personalized to the organization's own environment. Penetration testing is more manual, the expertise of the testers is more important and it is more complex and thus more expensive. [36][37] Both types of testing are needed as vulnerability scanning can be automated to be performed on shorter time frames and penetration testing is needed as ethical and non-ethical hackers can find critical vulnerabilities in systems that have had a vulnerability scan [37]. The topic "auditing methods" was split into these last two topics.

## **Incident Response Playbook – Cyber incident management, incident response, incident elevation**

A contingency plan is essential for an organization to quickly adapt and recover from known or unknown changes to the environment [38]. As part of a contingency plan, management needs to develop an incident response playbook that outlines the steps to take in event of a security breach and the steps to resolve it. The playbook should contain the steps necessary for who and under which circumstances to contact the incident response team, and when to elevate the issue to senior leadership and the criteria needed for incident elevation. The steps to meet regulatory obligations has to be included as well as the process by which management will contact its customers if needed, investors or other stakeholders. Lastly, the playbook needs to include steps on how an attack or breach would be isolated and mitigated as well as a review to prevent a similar attack in the future. The main responsibility of decision makers in the contingency process is to empower the people who would be in charge of the risk reduction measures as well as helping protect customer data and make sure the organization is in compliance with regulations [39]. It is critical for decision makers to make sure that the response playbook includes steps to remain in compliance with regulation and the process by which management will contact stakeholders. This topic covers aspects from cyber incident management, incident response, and incident elevation, aspects from these three where combined into this topic.

## **Cyberinsurance Coverage Components – Organizational security**

When dealing with risk mitigation, an organization has the option to opt for a risk avoidance measure. Cyberinsurance is a way to transfer the cost of a security breach to an insurer. Cyberinsurance works the same way as traditional insurance except that it normally has more coverage than just tangible property, as data is intangible. The four main components covered by cyberinsurance [40][41]:

1. Errors and Omissions: claims from errors in performance of a given service, negligence or product errors that cause customer data breach.
2. Multimedia liability: infringement of intellectual property like web defacement, liber, slander.

3. Network security and extortion liability: failure of network in case of malware, unauthorized access, loss of data confidentiality, business interruption (DDoS) and cyberextortion(ransomware)
4. Privacy management: Wrongful disclosure of personally identifiable information or confidential information, could include cost of investigation or services employed to lessen impact on customers like credit monitoring. Also includes loss of privacy through employee wrongfully handling data, human error, rogue employees, unencrypted communications and hacker getting access to data.

Decision makers could opt to contract cyber-insurance covering the components above as a method of risk transfer. Cyberinsurance was the most pervasive topic in organizational security.

### **Supply chain information security management and vendor selection process – Supply chain security**

When selecting vendors that will have access to customer confidential data, a risk profile based on pre-defined selection criteria to rank vendors by risk level is needed before management decides on using said vendor [42].

Supply chain security was divided into topics of selection criteria, vendor risk assessment and service level agreements (SLA).

The selection criteria [43] are based on attributes of the vendor: on-time response, logistics capability, overall quality, pricing and cost of the service being done by the vendor, how innovative they are, use of the latest technology, their facilities or assets and how flexible they are to adapt to the organization's needs. Management would then assign a numerical value range for each criterion and judge the vendor on the vendor's "grade" on each criterion. For example, the organization would assign the values of 1 for a timely response of less than one hour, 2 for response between 2-4 hours, 3 for response between 4-8 hours, 4 for response 8-24 hours, and 5 for response of more than 24 hours; the organization would then ask the vendor for previous incident reports or investigate how long the average response time is and assign its value. This process should be performed whenever the organization is looking to hire a third party and with existing vendors routinely.

A service level agreement (SLA) is an agreement between an organization with a vendor that defines the scope of the work and should include the security requirements set forth by the organization [42]. The SLA is supposed to be the foundation of the relation between the organization and the vendor [44]; as such, it should include the process by which the vendor will communicate breaches of a security requirement to the organization. The SLA should contain metrics by which the organization will audit the vendor such as incident numbers, time it took for responses, availability metrics, and other metrics that measure security performance [45]. The SLA should also contain enforceable stipulations for the organization to audit the vendor [46]. The specific provisions of the SLA need to be continually adjusted to best meet the organization's needs. It is not a simple process of creating the agreement once and not changing it, continual adjustments need to be made to the agreement [45].

Vendors need to be continually audited and monitored for compliance with security requirements after starting a business relationship with them [45]. Compliance methods should be identified in the SLA as well as the metrics needed to judge whether the vendor is in compliance. The audit should be held at a pre-arranged repeating time defined in the SLA, for example at the start of every fiscal quarter. If a vendor is failing to meet compliance requirements then it should be considered to replace the failing vendor [45].

### **Risk Assessment – Risk management, Cybersecurity asset management, Threat mitigation**

Risk management and cybersecurity asset management where combined here into organization's most valuable assets, asset valuation, CIA triad, risk = impact x probability, as well as including threat mitigation as risk mitigation strategies.

The corporate "crown jewels", the most critical assets, need to be identified as a first step in risk assessment for an organization. Management needs to know which assets are the most critical to protect when making decisions on how to spend the information security budget [47] [48]. The crown jewels must be included in the disaster recovery plan; the plan must center around recovering the assets, bringing them back online, or restoring any lost assets. Assets can be both an information system like software or a database or they could be data assets like customer personal information. Knowing what are the organizations most critical assets means that management can now focus their efforts and



investment in trying to best protect these assets and not spreading the investment evenly and thus less efficiently.

Along with the identification of the crown jewels, the less critical assets could be classified into different groups based on the criticality to the organization. Assets could be grouped into department or location so that management knows where to invest the most budget if it sees that most critical assets are grouped in a specific location. An asset inventory containing the asset and its risk classification and rank can be created and updated to have a centralized location where management can view their critical assets and support information.

The CIA triad stands for confidentiality, integrity, and availability and it is used as a basis for which to value IS assets. Confidentiality revolves around the principle of least privilege meaning that only a person with the correct authorization has access, viewing rights, or modification rights to an asset and not the rest of the public [49]. Integrity means ensuring an asset has not been tampered with at its different states; in-transfer, at rest, in-processing, or in-storage [49]. Availability means an asset is available for use and is accessible [49].

Each of the identified assets has a given “score” for each of the three CIA categories [50]. The score depends on the criticality of the asset in each of the three categories. The criticality is based on the impact the loss of each category has on the organization. An asset with a high availability score means that if the asset were to become unavailable then it would cause a high loss for the organization, while an asset with a low confidentiality score means that if the asset were to be accessed by someone without the required credentials it would cause a negligible or low cost to the organization. The scale of the score can be from a simple ranking of 0-3 or more complex to meet the organization’s needs, these numbers could also correspond to monetary values, e.g. 0 means 0-100 EUR, 3 means 100,000+ EUR so that the organization can place a monetary value on an asset’s CIA.

Risk is defined as the impact in losing confidentiality, availability, integrity times the probability it will happen ( $\text{Risk} = \text{Impact} \times \text{Probability}$ ) and can be classified from low to high level risks. As risk is not a simple vulnerability nor just the probability of a security event happening. Probability is the calculation of a vulnerability being exploited minus

the probability of a mitigating action [51]. Impact is the effect that a loss in an asset's CIA will have and includes a threat agent [51], it can be expressed in a monetary value or a simple score scale. A risk could be: a professional hacker hired by a competitor gains access to confidential blueprints exploiting a lack of encryption on an employee's laptop. The organization can calculate the probability of a competitor hiring a hacker as well as the probability of lacking encryption in employee computers, the customer's data has a confidentiality score. The probability can be expressed in a numeric value, 0-3, or more simple values, L = low / H = high, or a percentage probability.

Risk can then be classified between high to low or in percentage form, e.g. 50% probability and 100,000EUR impact. Management can then focus their efforts on deciding on which risks to spend the most investment in mitigating and which risks need less investment or attention.

Risks mitigation strategies can be classified as: avoidance, transfer/sharing, reduction, or retention [52].

Avoidance means that the organization will avoid the activity or asset that causes the risk, such as not allowing users ability to log in to web page or getting rid of a server. The use of this strategy is somewhat limited as it is not always practical or feasible to avoid performing a certain service or removing a certain asset. It could be useful in cases where an asset is high-risk prone and its risk classification outweighs the value it brings to the organization.

Risk transfer means the risk impact is transferred to a third-party. The risk still exists but it is a third-party who would be liable to the impact or a part of the impact. A common risk transfer strategy is cyber insurance. Not all the impact can be transferred, if a breach were to occur even if the organization has a risk transfer strategy, the organization is still liable for the loss of reputation.

Risk reduction means the reduction of the impact of a risk or its probability. Risk can be reduced by implementing security controls in the organization. Security controls could mandate that bans the use of personal computers in the workplace reducing the probability of an attacker gaining access to organization network. Security controls could also mandate for all e-mail communication to be encrypted thus reducing the impact of an email being seen by an unauthorized person.

Risk retention means the organization accepts the risk as the cost of the countermeasures to said risk are too high or the overall severity of the risk and its monetary loss is of little consequence to the organization.

Management needs to know how risk countermeasures relate to these four strategies when deciding on which risks to remediate and what measures they will use for risk remediation. These strategies are not mutually exclusive and a combination of them could be highly effective in mitigating risk.

### **Cyber Threats – IoT threats, APT, Human resources security, Types of threats/emerging risks**

Internet of things threats, advanced persistent threats, human resources security, and types of threats/emerging risks were combined into types of threats while leaving advanced persistent threats as its own topic.

Information security threats can be classified into external vs internal, human vs environmental vs technological, malicious vs non-malicious, and accidental vs intentional [53].

Management should be aware of the threats their organization faces; not all threats are the same. Management needs to understand the differences between the threat classifications as threat countermeasures vary depending on what kind of threat the organization is facing. Countermeasures aimed at deterring outside hackers might in fact increase the threat of internal non-malicious accidental threats. The classification breaks down the threat into source, agent, motivation, and intention so that it can be better understood:

- A. The source of the threat can be external or internal.
- B. The threat agent is classified as a human, the environment, or technology.
- C. The motivation can be malicious or non-malicious,
- D. In case of the threat agent being a human, the intention can be accidental or intentional.

Breaking down a threat into parts lets management better visualize their threat landscape as well as allowing them to better identify patterns which provides them with valuable information when deciding upon where and how to invest their security budget.

An advanced persistent threat (APT) is a threat that has a high level of expertise, significant resources, multiple attack vectors and whose objective is to exfiltrate intellectual property, undermine organization's critical missions, or to position itself to do carry these objectives in the future [54]. APTs act over an extended period of time and have the ability to adapt to the organization's countermeasures [54].

Management must be able to differentiate between a traditional threat and an APT as APT pose a much more serious risk to the organization and the resources needed to combat APTs are much greater. APTs differ from industrialized hacking as they're more personal where targets are more carefully selected, more persistent as the attacker is focused on gaining access to crucial systems or compromising intellectual property or sensitive information [55]. APTs only use a small degree of automation to enhance a focused attack, not to broaden an attack [55]. Only one threat agent is present in an APT [55]. APTs can manifest in different forms: nation-states aiming to steal intellectual property or establish influence in a specific region, corporations performing industrial espionage aiming to gain a competitive advantage by stealing intellectual property or sabotaging the competition, or criminals or terrorist organizations aiming to push a certain ideology or bring about societal change [56].

### **Cyber Security Training – Cybersecurity awareness and training**

This topic was left by itself as cyber security training.

Awareness education and training focused on the employees' roles and responsibilities are needed so that members of the organization can properly follow the organization's security policies and know how to fulfill their role and responsibilities [57].

While management is responsible for creating the organization's security policies, it is each of the organization's employee's responsibility to fulfill their roles. In order for the employees to be able to follow their roles, training and awareness education should be targeted to help employees follow the policies the organization created.

### **Security Policy Management – Cybersecurity policy creation, Security policy management**

Cybersecurity policy creation and management were combined into types of security policies, components and goals of a security policy, and security policy crafting process

There are three different kinds of security policy: regulatory, advisory, and informative [58].

Security policies can be broadly classified into the three categories, but policies within the three categories could be applied to the organization as a whole or to specific departments.

- A. Regulatory policies refer to policies required by governments or regulatory bodies typically present as legislation or standards. Management has little flexibility when dealing with regulatory policy as the organization must abide by these policies, however, exemptions may exist and management needs to be aware of their organization's status. When creating security policies, management needs to know which regulatory policies they need to follow and create security policies in their organization to comply.
- B. Advisory policies refer to policies written to provide recommendations clearly defining the actions to be taken or methods to use in defined situations. When writing advisory policies, management needs to know who they're writing the policy for as this kind of policy is aimed at individuals with the necessary knowledge to make decisions on how to act in the specified situation.
- C. Informative policies refer to policies which aim is to communicate information to a targeted audience. These kinds of policies are typically aimed at a larger audience and as such do not contain specific actions or methods, they mainly serve to inform an audience of a specific issue.

Knowing the policy classifications, management can assign a rank of importance to existing policies. Management can also better craft policy as they would know the goal of each kind of policy.

A security policy should be easy to understand, applicable, do-able, enforceable, able to be phased-in, proactive, avoid absolutes, and meet business objectives [58].

A successful security policy should contain all of the above distinctions. Since management is responsible for writing security policy, they should know the aspects of what makes a security policy successful. Management will not develop the documentation to follow a policy, they merely state what should be done not the specific technical aspects of how it should be done as such the policy needs to be clear so that the tactical decision

makers can craft the supporting documentation. Policies need to be applicable in order to be enforced; there is no use for a policy that is not applicable to the organization. Policies need to be applicable to different situations, therefore they should not include absolute values, instead they should have a degree of abstraction so that tactical decision makers can insert their own values into the policy. A proactive policy means it aims to deter a problem, prevent or mitigate an incident from happening.

The goals of security policies are to identify the organization's critical assets, identify potential risks, define the methods in which critical assets will be protected, define the methods in which incident reports or findings will be communicated, and define the way in which policies will be audited and reviewed [59].

Management needs to know the reasons why an organization needs security policies so that the crafted policies are effective. Security policies should mainly aim to protect the organization's "crown jewels"; policies should identify the critical assets and their corresponding vulnerabilities and threats. The methods by which the critical assets will be defended need to be covered by the policies. Reporting also needs to be covered by security policies, specifically how incidents are to be reported and to whom they will be reported. Lastly, policies should cover the process by which they will be reviewed so that management can change policies that are not effective or are not fulfilling the organization's business and security goals.

The crafting of security policies should follow a process of initial evaluation, development, approval, publication, implementation, and maintenance.

Management should know the process by which security policies are crafted so that it can follow the process to craft successful policies [58].

- A. The initial evaluation phase when the need for a security policy is submitted and management evaluates the request. At this stage it is decided if a security policy is needed.
- B. The development phase happens when management puts a team together to craft the policy, the technical requirements are presented and debated so that the team can agree on the final wording of the policy. At this point the policy could be tested.

- C. The approval phase is where management or the security policy committee receives the policy, discusses it, and decides on whether to approve it.
- D. The publication phase is when the policy is published to the organization or to the targeted audience/
- E. The implementation phase starts when the target audiences begins to implement the policy.
- F. The maintenance phase refers to the specified time when the policy is audited, its efficiency and necessity to the organization are reviewed to determine if the policy is fulfilling its intended goals and if the policy needs to be continued.

### **Business Continuity – Business impact, cybersecurity planning, business continuity, customer relationship management**

Business impact, cybersecurity planning, business continuity, and customer relationship management were combined into incident response plan, incident response team, business and disaster recovery plans and the process to create them, business continuity metrics, and backup strategies.

An incident response plan should define potential breach scenarios and steps in response, outline preventive measures, define stakeholder along with their roles and responsibilities, define communication and notification strategies, defines process for investigating incident and should defines methods to maintain business continuity [60] [61].

The main point of an incident response plan is to “minimize the duration and impact of security events” [60], as such a well-crafted plan is needed to make the incident process much smoother for the organization. Finding breach scenarios is part of risk management and vulnerability reviews, but the incident plan needs to include these risk scenarios and the steps the organization will take in case of an incident, along it should also contain the measures the organization is employing in order to mitigate those defined risks. The plan to communicate with the affected stakeholders also needs to be included as well as any strategies in dealing with other third parties such as the media to minimize the impact of an incident. The plan should also define the process by which the organization will resolve and investigate the incident and define who is responsible for investigating as well as defining roles for the investigation. Lastly, the plan should explain how to maintain

operations for the organization. Management is in charge of crafting, or to delegate the responsibility to a committee, the incident response plan and ascertain business goals are being followed so management needs to know what makes an incident response plan successful and what it should contain.

An incident response team should be comprised of a representative of senior leadership, a representative from the organization's IT or Cybersec team, a representative from the legal department, a representative from the communications or public relations department, and a representative from an external organization if necessary. [60] [62]

The incident response team contains representatives from different aspects of the organization to better fulfill the incident response plan.

- A. Senior leadership should oversee all actions of the team and oversees the team's adherence to the incident response plan and business and security goals.
- B. IT representative leads the investigation process and coordinates recovery efforts as well as providing vulnerability reviews and mitigation measures.
- C. Legal representative reviews any press releases to cover the organization legally as well as providing advice on liability issues and what information is communicated to affected parties.
- D. Public relations representative creates the press statements and is in charge of contacting the media as well as the methods by which the organization will contact stakeholders and media, they are also responsible for assessing the reputation impact from an incident.
- E. External organization representative's main responsibility is to provide expertise that the organization lacks and needs for the incident, such as forensic investigations or regulatory issues.

When adding employees to the incident response team, management needs to know the different sectors of the company that need to be represented and their responsibilities so that the most efficient team can be created to oversee the deployment of the incident response plan.

A business continuity plan is composed by: business impact analysis, disaster contingency recovery plan, and training and testing strategy. [63]



Business continuity and IT security planning have become more integrated in recent years and corporate leadership is increasingly responsible for business continuity planning [63] as such management needs to know the components of a continuity plan to craft an effective and comprehensive business continuity plan that covers IT risks.

- A. Business Impact Analysis main purpose is to identify the business-critical functions and their associated risks as well as ranking the risks based on probability of happening and impact an incident will have on the enterprise.
- B. Disaster contingency recovery plan outlines the procedures the organization will take to return to working state in case of an incident occurring.

Training and testing strategy is meant to continually test the disaster recovery plan to ascertain the recovery teams know how to act in case of an incident and develop confidence as well as reassessing the business impact analysis to ascertain it covers the most critical risks

The process to create a business continuity and disaster recovery plans is to develop the contingency planning policy statement, conduct a business impact analysis, identify preventive controls, develop recovery strategies, develop an IT contingency plan, testing of the plan and training of employees, and maintenance of the plan. [64][65]

Management is ultimately responsible in case of an incident, whether it be legally liable or liable to the stakeholders, as such management needs to know the process to create a business continuity and disaster recovery plan so that they can take an active part in the crafting of the plan and to provide support to the security teams delegated to create the details of the plans [64].

- A. Contingency planning policy statement should reflect the organization's overall objectives and establish the overall framework and responsibilities so that all personnel can understand the organization's contingency planning requirements [65].
- B. A business impact analysis(BIA) correlates a given system with a business process or goal and calculates the cost of a disruption given the relation between the two. It can then be used to for planning of contingency requirements and priorities. [65]

- C. Identification of preventive controls - Impact from a disruption identified in the BIA can be mitigated or eliminated by preventive measures [65]. These measures are identified at this step of the process.
- D. Creation of IT contingency and recovery strategies – in case preventive controls fail to mitigate a disruptive event, strategies need to be created to define the process of backup and recovery through a disaster recovery plan. [65] The plan needs to identify the backup and recovery strategy as well as the backup methods and where the backup data is stored. It should also define the incident response team. [65]
- E. After the different plans and strategies are created, testing must be done to identify the capabilities of the plans and their deficiencies. Testing should be done in an environment closely resembling the live production environment. The training of personnel should focus on getting them acquainted with their roles and teaching them the skills to fulfill their roles in the contingency plans. The organization could also hold tabletop or functional exercises to further familiarize personnel to their roles and responsibilities. [65]

The business continuity and disaster recovery plans need to be reviewed, changed and maintained at regular intervals and when significant changes occur.

The two key measures when dealing with disaster recovery are recovery time objective (RTO) and recovery point objective (RPO). [66]

- A. The recovery time objective refers to the duration of time in which key business functions are unavailable and must be restored [66]. It is also the time by which functions need to be restored before causing unacceptable damage due to a lack of functionality [67]. It designates how much time can pass in case of a disruption before the organization faces serious consequences.
- B. The recovery point objective refers to the time between two backups of data or the time needed for an unacceptable quantity of data to be lost [66][67]. It can be thought of as the organization's tolerance to disruption or how much data can be lost due to a disruption before the organization's losses exceed the planned amount.

RTO is measured in time while RPO can be measured with a monetary value. Management needs to know how a disaster recovery plan is measured to be able to understand it. Since RPO directly deals with business goals, management also needs to know this measurement as they need to set the threshold of how much can be lost so that the disaster recovery plan can include it on the RPO measurement.

A system backup option can be placed onsite, co-located, or on the cloud and can be in a state of hot, cold, or warm [66].

A backup should not be placed in the same physical location as the primary system [66], as such the organization has the option to place the backup in a co-location meaning somewhere remotely or in the cloud. The organization could also choose to accept the risk and place the backup onsite having both primary and backup in the same location. Each of the three options will impact the cost of maintaining a backup as such management needs to know the different options available to them to make the most financially sound decision for their organization.

A backup can be in different states: cold, hot, or warm. A cold state means that hardware, software, or applications would need to be installed for a backup to come online, meaning it could take hours or days for the system to become operational again. A hot state means the backup can come online in a matter of seconds or minutes and has the capability to take over primary processed from the primary system and has no need for any hardware or software installations for it to become operational. A warm state refers to a state between hot and cold and is less defined. Each of these states carry different costs, a cold state is much cheaper than a hot state, Management needs to know their options to consider the costs when deciding upon a backup strategy.

### **Cybersecurity committee – Cybersecurity committee**

The main responsibilities of the cybersecurity committee are to decide on risk ownership, making sure proper controls are implemented, overseeing the adherence to a regulating framework, overseeing the cybersecurity budget, making sure there is a proper incident response plan, and the disclosure of information to stakeholders. [68]

It is management's responsibility to delegate risk oversight to a cyber security committee and management takes an active part in said committee so they should know what the responsibilities of the committee are so that they can make informed decisions on the committee's makeup.

- A. Risk ownership refers to the employee who owns the risk and the impact the risk could have as well as including a vulnerability assessment.
- B. Proper controls being implemented refers to the committee making sure that identified risks have proper controls implemented designed to mitigate the probability and impact of the risk.
- C. Adherence to a regulating framework refers to the committee ascertaining that the organization follows a security framework such as NIST or ISO and how the organization's current operations compare to the industry standard.
- D. Budget oversight refers to the committee making sure the organization has the appropriate budget to fulfill the organization's information security objectives as well as how effective the current budget is.
- E. Oversight over incident response refers to making sure there is an incident response and business continuity plan in place as well as the organization's preparedness to follow the continuity plans.

Oversight over disclosure refers to the ability for the organization to contact customers or stakeholders in case of disruptions or breaches. The topic cybersecurity committee was not combined or divided.

### **Development Process – Secure software development**

Secure software development topic was divided into secure software development and secure software development lifecycle model.

The security development lifecycle has seven phases: training, requirements gathering, design, implementation, verification, release, and response. [69]

Management oversees the selection of personnel [70] who will lead and the teams in charge of designing and implementing the software project so it is vital management knows the different steps to securely develop software. Knowing the process will also

allow management to more efficiently communicate with CISOs or the security team as to the status of the project or any questions regarding security concerns.

- A. Training phase – in this phase the different personnel who will be working on the project are given core security training into how to build more secure software.
- B. Requirements gathering phase – in this phase the security requirement are defined, it is one of the first goals in the project. At this phase acceptable levels of quality are also established as well as the initial risk assessments are performed.
- C. Design phase – design requirements are developed and the attack surface is analyzed. Along with software design modeling documents, threat modeling is also documented.
- D. Implementation – software is developed using approved tools. Code is analyzed and reviewed.
- E. Verification – Checks are done to the running program to monitor for issues. Program is tested by introducing malformed data to reveal unforeseen errors. Attack surface is once again reviewed.
- F. Release – Incident response plan is created or updated, final security review is done, software is then certified to make sure requirements were met.
- G. Response – Incident response plan is executed in case of incidents.

## 5. Survey Elaboration

This section will discuss the elaboration of the survey, which tool was used, how the cards were presented and will discuss how participants would see the survey.

### 5.1 Survey Tool

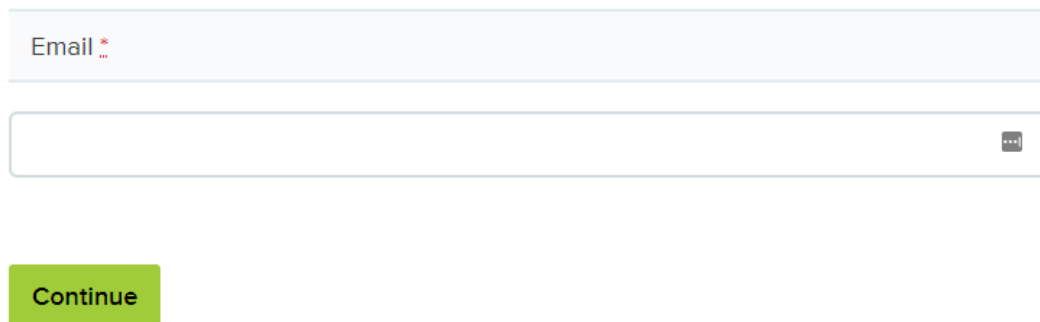
The tool chosen to deliver the survey was Optimal Sort web tool for Card Sort. The reasons for choosing this tool was the ease to develop the survey, the ease of which participants could partake, and the ability to include descriptions for each card. Survey participants needed to simply follow a web link to access the survey: <https://3p7la235.optimalworkshop.com/optimalsort/mru46a6y>. The links were delivered through email or Facebook conversation to the participants.

The first screen the participants would see if the welcome message and asking for participant email.

### Welcome to this study.

Thank you for agreeing to participate!

The activity shouldn't take longer than **15 to 30** minutes to complete.



Email \*

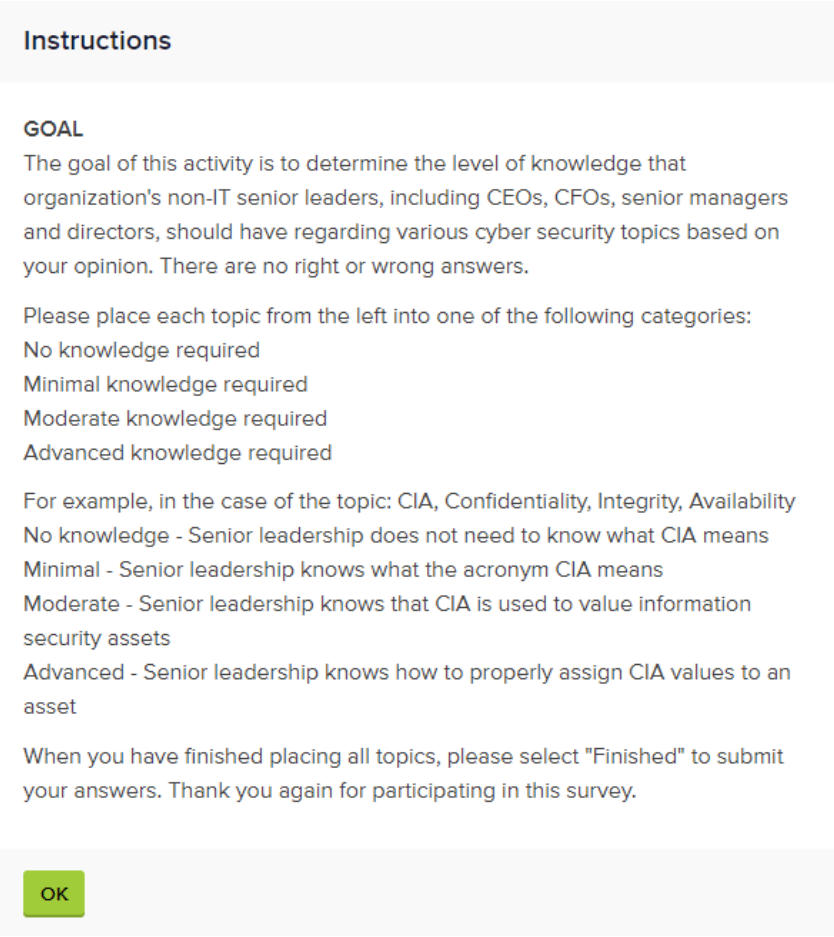
Continue

Figure 3. Welcome Screen

The survey was pilot tested on 3 individuals with knowledge ranging from novice in cybersecurity to more advanced knowledge. The pilot test was meant to test for clarity in wording as well as clarity in the instructions. The first find of the pilot survey was that the average time to completion was around 20 minutes which is why the activity time was

chosen as 15 to 30 minutes. This was also included as to not rush participants to finish quicker.

After participants would insert their email and click the continue button, the instructions screen would be displayed.



**Instructions**

**GOAL**

The goal of this activity is to determine the level of knowledge that organization's non-IT senior leaders, including CEOs, CFOs, senior managers and directors, should have regarding various cyber security topics based on your opinion. There are no right or wrong answers.

Please place each topic from the left into one of the following categories:

- No knowledge required
- Minimal knowledge required
- Moderate knowledge required
- Advanced knowledge required

For example, in the case of the topic: CIA, Confidentiality, Integrity, Availability

- No knowledge - Senior leadership does not need to know what CIA means
- Minimal - Senior leadership knows what the acronym CIA means
- Moderate - Senior leadership knows that CIA is used to value information security assets
- Advanced - Senior leadership knows how to properly assign CIA values to an asset

When you have finished placing all topics, please select "Finished" to submit your answers. Thank you again for participating in this survey.

OK

*Figure 4. Instructions*

The GOAL section of the instructions is meant to immediately communicate the purpose of the survey to the participants so as to get them in the right frame of mind to categorize the cards. Since the goal is to find what the participants think, the sentence “There are no right or wrong answers” was included to not make them feel cajoled to a certain answer.

The instructions also define the different categories in which the participants will sort cards into: No knowledge, minimal knowledge, moderate knowledge, and advanced knowledge. Initially, the terms low-level, medium-level, and high-level knowledge were chosen but with feedback from the pilot survey it was then changed. Feedback pointed out that it would be difficult for participants to equate what low-level knowledge of a

certain topic means. It could mean having knowledge only of lower-tier operations, meaning tactical knowledge, or just not having much knowledge on the topic. Minimal, moderate, and advanced were chosen as they reflect the purpose of the survey the most clearly. Since the main goal is to find what knowledge should non-IT senior leaders have, the survey includes the option of no knowledge so that participants can point out topics in which senior leaders should have no knowledge of but also define what level of knowledge should senior leaders have. A topic could also be categorized as minimal knowledge required meaning that less focus should be placed on this topic. Topics ranked no-knowledge and minimal knowledge would indicate that these topics are not critical to senior leaders while moderate and advanced knowledge topics would be the most critical.

Since minimal, moderate, and advanced knowledge rely on the participant's understanding and opinion of what each means for each topic, a disambiguation of a topic was provided as an example so that participants would be able to more clearly understand how to think of each topic. The topic of CIA was chosen as an example as it refers to a specific meaning and not a security operation like risk assessment. This was done so that participants would understand that knowledge does not only mean knowing what a topic means but also its usability, applicability, and roles and responsibilities associated with it. Minimal knowledge means solely knowing what a topic means or having general awareness of said topic, so the corresponding meaning in the example is knowing what the acronym means. Moderate knowledge means having knowledge of how the topic is used, applicability, so the corresponding description is knowing that CIA is used to value information security assets. Advanced knowledge means having knowledge of how to use the topic, not just how it's used, as well as roles and responsibilities associated with it so the corresponding example is knowledge on how to value assets using CIA.

Figure 5 displays how the survey is visible to participants. The image shows one card in each category. The cards are displayed on the left side and participants can easily drag and drop each card into one of the four categories. The I symbol next to each card allows the user to click on it to display the comment associated with the card. The comments mainly serve to further explain what the card is by providing a brief description or explanation of the topic. There is no timer on the web view, but the number of remaining cards is shown at the bottom (not shown in figure). Each category shows how many cards



are grouped into it. All cards are required to be sorted and the cards always are displayed in the same order. There is no limit to the number of cards allowed in each category.

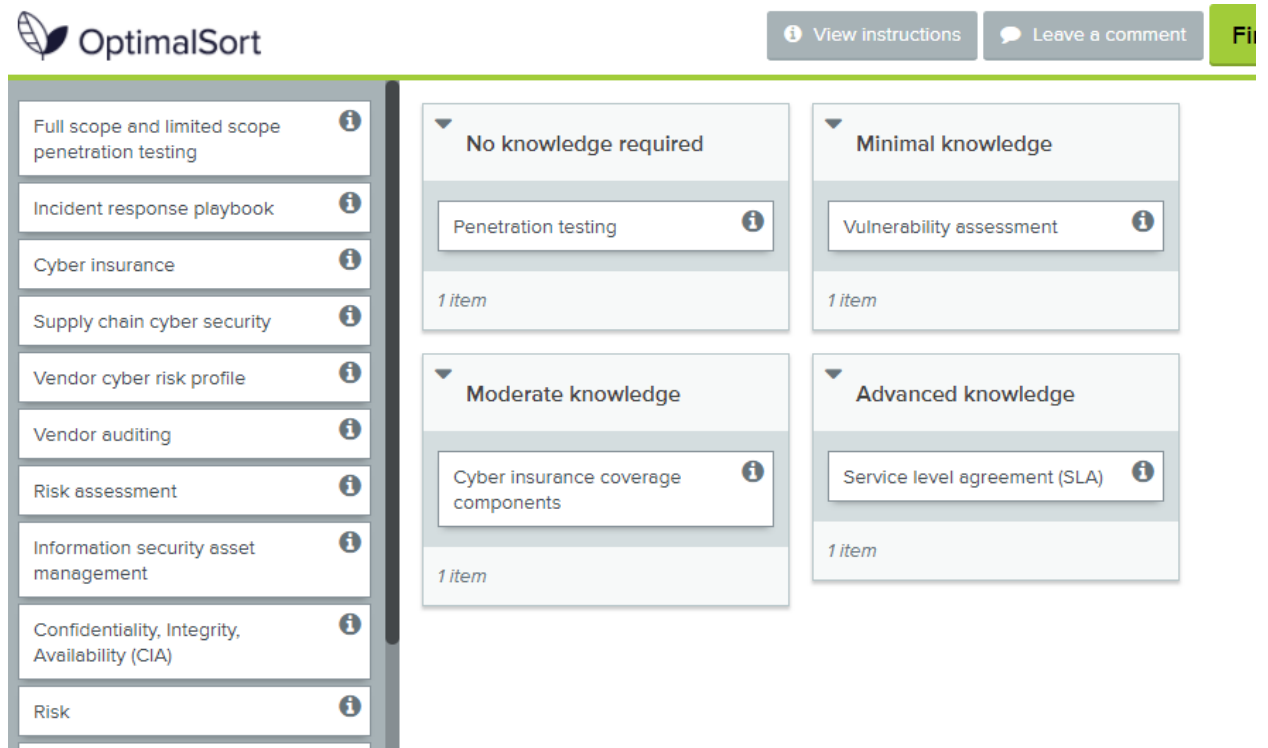


Figure 5. Survey Example

## Thanks

All done, awesome! Thanks again for your participation. Your feedback is incredibly useful!  
You may now close this window or navigate to another web page.



Figure 6. Survey End

Figure 6 displays the goodbye message of the survey. The results are then sent through e-mail in a json format. The format: `JSON{["Card Number": 1-4 ]}`. Each card has an associated index number to it which is displayed in a list in the JSON response with a number from 1 to 4. The numbers correspond with each of the categories: 1-No knowledge, 2-Minimal, 3-Moderate, 4-Advanced.

## 5.2 Card List

There is a total of 43 cards derived from the descriptions section. Each card has an index number, followed by the topic name which is displayed to participants, and the description which is displayed when the I icon is clicked.

Label	Description
C1. Penetration testing	Process of performing authorized simulated attacks on a computer system used to evaluate the system's security
C2. Full scope and limited scope penetration testing	Limited scope = limiting access to testers   Full scope = testers have unlimited access to systems
C3. Vulnerability assessment	Process of identifying vulnerabilities in a system using widely available tools
C4. Incident response playbook	Playbook that outlines the steps necessary to contact incident response team, guide on elevating incidents to senior management and criteria for elevating incidents
C5. Cyber insurance	Insurance used to protect organization against information technology related risks
C6. Cyber insurance coverage components	Components covered by cyber insurance: errors and omissions, multimedia liability, network security and extortion liability, privacy
C7. Supply chain cyber security	Process to ensure cyber security in the organization's supply chain
C8. Vendor cyber risk profile	A risk profile based on pre-defined selection criteria used to rank vendors by cyber risk level
C9. Service level agreement (SLA)	An agreement between an organization with a vendor that defines the scope of the work and should include the security requirements set forth by the organization
C10. Vendor auditing	Process of auditing vendors and monitoring for compliance with security requirements
C11. Risk assessment	Process of identifying potential risks to organization's assets
C12. Information security asset management	Process of identifying organization's assets and ranking assets in terms which are most critical for the organization
C13. Confidentiality, Integrity, Availability (CIA)	Parameters by which to value assets
C14. Risk	Impact of losing confidentiality, availability, or integrity times the probability it will happen, Risk = Impact x Probability
C15. Risk mitigation strategies	Avoidance, transfer/sharing, reduction, retention

C16. Information security controls	Countermeasures to avoid or reduce risks
C17. Cyber threats	Any threat to the organization's assets or information systems
C18. Types of cyber threats	Threats can be human or environmental, malicious or non-malicious, accidental or intentional
C19. Advanced persistent threat (APT)	A threat that has a high level of expertise, significant resources, multiple attack vectors and whose objective is to exfiltrate intellectual property, undermine organization's critical missions, or to position itself to carry these objectives in the future
C20. Security policies	Policies aiming to explain how organization will protect its assets
C21. Types of security policies	Regulatory, advisory, informative
C22. Security policy creation	Understanding of security policy goals, successful aspects of a security policy, and process for creating policy
C23. Information security incident	Successful or unsuccessful attempt of unauthorized use or access of information
C24. Incident management	Process to identify, analyze, and solve incidents in the organization
C25. Incident response plan	Plan that defines potential breach scenarios and steps in response along with roles and responsibilities of stakeholders
C26. Incident response team	Makeup of team, roles and responsibilities, as well as goals
C27. Business continuity plan	Composition of plan: business impact analysis, disaster recovery plan, training and testing strategy
C28. Business continuity planning	Process to create business continuity and disaster recovery plans
C29. Disaster recovery plan	Plan that defines steps to be taken if an incident which affects business continuity occurs
C30. Recovery time objective (RTO)	Target amount of time a system can be inoperative
C31. Recovery point objective (RPO)	Maximum target period of time in which data can be lost due to incident
C32. Disaster recovery planning	Process to create disaster recovery plan, recovery planning steps, and process to execute plan
C33. Backup strategy	Backups onsite, co-located, cloud and backup state hot, cold, or warm
C34. Cybersecurity committee	Makeup, goals, and responsibilities of committee (decide on risk ownership, oversee adherence to framework, etc)
C35. Secure software development	Best practices and software security testing

C36. Secure software development life cycle (SSDLC)	Model like MS Security development lifecycle
C37. Cyber security framework	Framework such as ISO 27001 or NIST 800-53 as well as compliance to framework
C38. Human resources security	Define employee security roles and responsibilities, employee screening, disciplinary process, employee termination process
C39. Cyber security training	Cyber security awareness education and training focused on employee roles and responsibilities
C40. Access controls	Controls aimed at allowing only authorized access to system or data, includes identification, authorization, authentication and approval
C41. Access control models	Discretionary access control, mandatory access control, role-based access control
C42. Operational security (OPSEC)	Process of identifying assets to protect, identifying threats, analyzing vulnerabilities, risk assessment, and implementing controls and countermeasures
C43. Cryptography	Practice of securing communications to prevent third party from reading or gaining data

*Table 2. Card List*

Initially, each card included the topic as seen above but the description was different. The description included suggested examples of ranking of what minimal, moderate, and advanced meant for each topic. The pilot survey identified this as an area of confusion as the participants commented that the display was too cluttered and hard to understand if every topic had its own ranking. It was also mentioned that it took significantly longer to complete as participants spent more time reading cards instead of categorizing them. If the ranking for each card were to be included, then the participants could mistakenly categorize the cards depending on if they agree on my assessment on what constitutes minimal or moderate knowledge as it pertains to every topic, which is not the goal of the survey. It is also outside the scope of the study to previously define what each ranking means for each category. For these reasons, the cards were changed to display a brief description of the topic and allow the participants to devise their own definitions of what constitutes minimal or moderate knowledge.

The pilot survey was administered to three individuals. The individuals were chosen as they were willing to assist with the survey development and have some knowledge in the field of cyber security. They were given the survey just as a participant but they took the survey while on a Skype call so they could voice their recommendations and comments.

Card 1 (Penetration testing) was also categorized as no-knowledge. Since penetration testing is a complicated and technical process, it can be deduced some participants believed it was out of the realm of senior leaders.

## 6. Results

This section will discuss the results of the survey.

### 6.1 Raw Results

Table 3 displays the raw results of the survey. The first column contains the card with its index number as it corresponds in Table 2. The next four columns are for each of the categories. In each cell in the matrix there is a percentage indicating the percent of times a card was sorted into the category.

Card Number	No Knowledge	Minimal	Moderate	Advanced
C1. Penetration Testing	20%	30%	20%	30%
C2. Full scope and limited scope penetration testing	0%	40%	40%	20%
C3. Vulnerability Assessment	0%	40%	30%	30%
C4. Incident response playbook	0%	40%	30%	30%
C5. Cyber insurance	0%	30%	40%	30%
C6. Cyber insurance coverage components	0%	50%	20%	30%
C7. Supply chain cyber security	0%	50%	30%	20%
C8. Vendor cyber risk profile	0%	30%	60%	10%
C9. Service level agreement (SLA)	0%	60%	20%	20%
C10. Vendor auditing	0%	50%	50%	0%
C11. Risk assessment	0%	40%	20%	40%
C12. Information security asset management	0%	50%	40%	10%
C13. Confidentiality, Integrity, Availability	0%	50%	40%	10%
C14. Risk	0%	50%	20%	30%
C15. Risk mitigation strategies	0%	40%	50%	10%
C16. Information security controls	0%	30%	30%	40%
C17. Cyber threats	0%	30%	60%	10%
C18 Types of cyber threats	0%	30%	50%	20%
C19. Advanced persistent threat (APT)	0%	20%	40%	40%

C20. Security policies	0%	10%	80%	10%
C21. Types of security policies	0%	30%	60%	10%
C22. Security policy creation	0%	20%	70%	10%
C23. Information security incident	0%	30%	40%	30%
C24. Incident management	0%	40%	30%	30%
C25. Incident response plan	0%	30%	60%	10%
C26. Incident response team	0%	40%	40%	20%
C27. Business continuity plan	0%	40%	40%	20%
C28. Business continuity planning	0%	30%	50%	20%
C29. Disaster recovery plan	0%	20%	60%	20%
C30. Recovery time objective (RTO)	0%	50%	30%	20%
C31. Recovery point objective (RPO)	0%	40%	20%	40%
C32. Disaster recovery planning	0%	0%	90%	10%
C33. Backup strategy	0%	50%	20%	20%
C34. Cybersecurity committee	20%	20%	30%	30%
C35. Secure software development	0%	50%	20%	30%
C36. Secure software development life cycle (SSDLC)	0%	40%	50%	10%
C37. Cyber security framework	0%	80%	0%	20%
C38. Human resources security	0%	60%	10%	30%
C39. Cyber security training	0%	60%	0%	40%
C40. Access controls	0%	60%	30%	10%
C41. Access control models	20%	50%	20%	10%
C42. Operational security (OPSEC)	20%	40%	20%	20%
C43. Cryptography	20%	40%	10%	30%

*Table 3 Raw Survey Results*

Without needing to do in-depth analysis, trends appear from the raw data overview. We can see that the no knowledge required category was the least picked category for most cards while the minimal and moderate categories were the most picked. Several cards had a wide consensus of participants agreeing in its categorization, for example the 90% moderate in card 32 or 80% minimal on card 37. There are also cards where opinion is much more split, for example on card 4 having 40% minimal and 30% for moderate and advanced.

It was unexpected that many participants chose to not categorize many cards into the no knowledge category. Since the example given in the instructions mentioned that minimal knowledge meant only having general awareness of a topic, it is somewhat reasonable to believe that participants would believe that senior leaders should have at least general awareness of all topics listed. No topics were categorized mainly as no-knowledge but some did receive 20% categorization in the no knowledge category. These topics mainly deal with technical aspects, as is the case with 42(Operational Security) and 43(Cryptography). Card 41 (Access control models) was also ranked as no-knowledge, probably due to the fact that the specific models for access controls are more technical information that senior leaders don't need to be aware of.

Cybersecurity committee card (C34) also received a no-knowledge categorization 20% of the time but was also ranked in the advanced and moderate categories 30% of the time each. This could be because participants believe senior leaders should not be part of the cybersecurity committee. It could also be due to participants being CISOs and believing that the cybersecurity committee is their realm of work and senior leaders should not interfere.

## **6.2 Best Merge Method**

The best merge method (BMM) aims to count the number of incidences of pairings in a card sort activity [29], a pairing in this case is a topic paired with one of the four provided categories. In an open card sort activity, when participants are allowed to create their own categories, the BMM would find the frequency of pairings and find the most frequent pairs in all groups. New groups would then be constructed from the most frequent pairs. Since the card sort activity for this study was closed, the new groups created were for those topics which received equal matches in two or more categories. Along with the four categories in the survey, the new groups are minimal-moderate, minimal-advanced, and moderate-advanced. This method does not take into consideration that the categories act as a scale so might not represent a full view on the results, as such a topic categorized 40% advanced and 60% minimal would have its best match be the minimal. Another method to analyze cards would be the Actual Merge Method[29], this method looks at whole groups and finds the number of instances of a complete group, or how many times were specifically topics A, B, C grouped in category 1. Since the study is more interested



in where the topic was categorized and not on how many topics were included in each category the BMM was chosen.

Table 4 displays the results from the survey using the best merge method. Using this method we rank the cards by which pairings had the most incidence percentage in. The purpose of this analysis is to display which topics were most associated with each of the four categories. This initial analysis gives us information of which topics could be the most important for senior leaders to know about.

<b>Card</b>	<b>No</b>	<b>Minimal</b>	<b>Moderate</b>	<b>Advanced</b>
C37. Cyber security framework	0	80	0	20
C39. Cyber security training	0	60	0	40
C38. Human resources security	0	60	10	30
C9. Service level agreement (SLA)	0	60	20	20
C40. Access controls	0	60	30	10
C33. Backup strategy	0	60	20	20
C14. Risk	0	50	20	30
C35. Secure software development	0	50	20	30
C7. Supply chain cyber security	0	50	30	20
C30. Recovery time objective (RTO)	0	50	30	20
C6. Cyber insurance coverage components	0	50	20	30
C12. Information security asset management	0	50	40	10
C13. Confidentiality, Integrity, Availability (CIA)	0	50	40	10
C41. Access control models	20	50	20	10
C3. Vulnerability Assessment	0	40	30	30
C4. Incident response playbook	0	40	30	30
C24. Incident management	0	40	30	30
C43. Cryptography	20	40	10	30
C42. Operational Security (OPSEC)	20	40	20	20
C10. Vendor auditing	0	50	50	0
C2. Full scope and limited scope penetration testing	0	40	40	20
C26. Incident response team	0	40	40	20

C27. Business continuity plan	0	40	40	20
C32. Disaster recovery planning	0	0	90	10
C20. Security policies	0	10	80	10
C22. Security policy creation	0	20	70	10
C8. Vendor cyber risk profile	0	30	60	10
C17. Cyber threats	0	30	60	10
C21. Types of security policies	0	30	60	10
C25. Incident response plan	0	30	60	10
C29. Disaster recovery plan	0	20	60	20
C15. Risk mitigation strategies	0	40	50	10
C36. Secure software development life cycle (SSDLC)	0	40	50	10
C18. Types of cyber threats	0	30	50	20
C28. Business continuity planning	0	30	50	20
C5. Cyber insurance	0	30	40	30
C23. Information security incident	0	30	40	30
C11. Risk assessment	0	40	20	40
C31. Recovery point objective (RPO)	0	40	20	40
C19. Advanced persistent threat (APT)	0	20	40	40
C34. Cybersecurity committee	20	20	30	30
C16. Information security controls	0	30	30	40

*Table 4 Best Merge Display*

From the best merge display can be accurately see that the most recurring pairings are in the minimal category and moderate category. Table 4 has grouped the topics into six different categories, all marked with a different color. The first category shown is the minimal knowledge category. This represents all the topics in which senior leaders should only have a general awareness of. The topic with the most agreeance on in this category was C37-Cyber security framework. We can also see that C39-Cyber security training was agreed on the minimal category 60% of the time but also on the advanced category 40% of the time. This could be due to participants believing that training should be left to the security professionals and senior leaders only being aware of what kind of training is being given in the organization.

The next category represents topics in which the percentage for minimal and moderate was the same. These include C2-Full scope and limited scope penetration testing and C10-Vendor auditing. Both topics represent auditing methods for an organization while C2 being more technical and C10 less so. Since senior leaders are not expected to perform penetration tests or perform the vendor audit themselves and they are involved in making decisions on selecting vendors, it is reasonable to believe that senior leaders should have an awareness of what the two are but also know how they are used. Participants were split between general minimal and moderate. Cards C26-Incident response team and C27-Business continuity plan were also categorized as a tie between minimal and moderate. The literature recommends [34] that senior leaders should be engaged in the incident response team so the moderate categorizations could stem from this belief while other participants might believe senior leaders should not be part of the incident response team and merely know if their organization has one. For C27. Business continuity plan, the minimal categorizations could stem from senior leaders knowing there is a plan in place while not needing to know the details, the moderate category would mean that senior leaders know the details of how the plan would be set in motion in case of incidents.

The next category represents the topics ranked in the moderate category. The most agreed upon topics were C32-Disaster recovery planning, C20-Security policies, and C22-Security policy creation. Of note in this category is that disaster recovery planning was ranked 90% moderate and 10% advanced while disaster recovery plan was ranked only 60% moderate, 20% advanced but also 20% minimal. One of the participants could believe that the role of senior leaders in disaster recovery planning is the creation of the disaster recovery plan while others would believe that it is more important for senior leaders to be engaged in the actual steps of the plan more so than the writing of the plan. We can see this same thinking repeated with the topics C27-Business continuity plan and C28-Business continuity planning. This points towards a trend of senior leaders being engaged in planning is more important than senior leaders being part of the writing of the plan or knowing how the plan works and is applied.

Topics C20-Security policy and C22-Security policy creation were also agreed highly on the moderate category. The two topics pertain to the same general idea, security policies. The third topic C21-Types of security policies was highly ranked in moderate with a 60%

instead of 80% or 70%. This points to the general topic of security policies being important knowledge that is relevant for senior leaders to be knowledgeable in.

The next category represents topics which were split between minimal and advanced, this category can be thought of as contentious topics or topics in which there is significant disagreement. These topics include C31-Recovery point objective and C11-Risk assessment. For C11-Risk assessment some of the literature recommends [71] that senior leaders only be aware of the most significant assets the organization has while other parts of the literature recommend [56] for senior leaders to know their major risks as well as assets and how those risks affect the organization. Both of these lines of thinking can be seen on the survey results as some participants are indicating that senior leaders only have general awareness of risk assessment while other believe senior leaders should take an active role and know how risk assessments are made and how the assessment is used to fortify the organization. C31-Recovery point objective is an interesting selection for this contentious category. The topic mainly deals with disaster recovery and is included in the disaster recovery plans, which was also ranked in the minimal category so that minimal ranking could stem from there. The topic also represented the maximum amount of data that can be lost which would be a business decision meaning that senior leaders should be very involved in understanding how much data can the organization afford to lose and where and how this number would be used in disaster recovery planning. This also correlates to participants believing that senior leaders should focus on planning and not on the plans themselves.

The next category represents topics that were split between moderate and advanced. The first topic is C19-Advanced persistent threat (APT), this categorization was not very surprising as the literature specifically mentions senior leaders needing to be aware of the organizations greatest threats and naming or describing what APTs are. The more interesting topic is C34-Cybersecurity committee, this topic was split 30% for moderate and advanced but also 20% for no knowledge and minimal. It is interesting because very few topics and a score of greater than 0 in no knowledge and this topic seems to have no agreement on. This could be that participants are split on believing whether non-it senior leaders should participate or be part of an organization's cybersecurity committee.

The last category is that in which topics were ranked in the advanced category the most. The only topic in this category is C-16 Information security controls, it is only ranked

40% for this category indicating a not very strong inclination to advanced knowledge. This could be due to security controls being a part of general user information security training as such being important information senior leaders should know. The description included was “countermeasures to avoid or reduce risks”, so since senior leaders oversee the decision-making process they would have the final word on which countermeasures would be implemented.

## 7. Summary

This final section will provide a list of topics with their corresponding average score from the survey and incidence rate in the literature. The average score is calculated by assigning a value to each category in the survey (No knowledge =1, Minimal =2, Moderate =3, Advanced =4) and calculating the average score for each topic. Each topic was categorized 10 times, 10 different participants, the average was calculated by:

$$\frac{1a + 2b + 3c + 4d}{x}$$

Where a = number of no knowledge incidences, b = minimal, c = moderate, and d = advanced. X is the number of participants, in this case 10. This was done for every card and displayed in the table below.

*Table 5 Summary of Results*

Topic	Average	Incidence
C19. Advanced persistent threat (APT)	3.2	5%
C16. Information security controls	3.1	25%
C32. Disaster recovery planning	3.1	40%
C5. Cyber insurance	3	15%
C11. Risk assessment	3	85%
C20. Security policies	3	35%
C23. Information security incident	3	50%
C29. Disaster recovery plan	3	40%
C31. Recovery point objective (RPO)	3	35%
C3. Vulnerability assessment	2.9	35%
C4. Incident response playbook	2.9	50%
C18. Types of cyber threats	2.9	30%
C22. Security policy creation	2.9	45%
C24. Incident management	2.9	50%
C28. Business continuity planning	2.9	40%
C2. Full scope and limited scope penetration testing	2.8	35%
C6. Cyber insurance coverage components	2.8	15%

C8. Vendor cyber risk profile	2.8	35%
C14. Risk	2.8	40%
C17. Cyber threats	2.8	30%
C21. Types of security policies	2.8	35%
C25. Incident response plan	2.8	45%
C26. Incident response team	2.8	45%
C27. Business continuity plan	2.8	40%
C35. Secure software development	2.8	5%
C39. Cyber security training	2.8	45%
C7. Supply chain cyber security	2.7	35%
C15. Risk mitigation strategies	2.7	25%
C30. Recovery time objective (RTO)	2.7	35%
C34. Cybersecurity committee	2.7	40%
C36. Secure software development life cycle (SSDLC)	2.7	5%
C38. Human resources security	2.7	30%
C1. Penetration testing	2.6	35%
C9. Service level agreement (SLA)	2.6	35%
C12. Information security asset management	2.6	60%
C13. Confidentiality, Integrity, Availability (CIA)	2.6	85%
C33. Backup strategy	2.6	15%
C10. Vendor auditing	2.5	35%
C40. Access controls	2.5	5%
C43. Cryptography	2.5	5%
C37. Cyber security framework	2.4	45%
C42. Operational security (OPSEC)	2.4	5%
C41. Access control models	2.2	5%

The averages table gives us a different view on the results, by calculating the average with can rank the topics against each other on the same scale as well as comparing them to the literature incidence rate. A higher average means participants mostly selected the

topic as higher knowledge required so the topics can be ranked from highest to lowest average to rank them in level of importance. Training programs can use the list provided by Table 5 to select which topics to mostly focus on in training programs for senior leaders.

The lowest average in the list is 2.2 while the highest is a 3.2. The topic with the 3.2 average was Advanced Persistent Threat (APT) while the topic with 2.2 average was access control models. The average among the topics was a 2.77, being both 5 points from 2.2 and 3.2, meaning that topics with an average score lesser than 2.77 are those which were consistently ranked of lesser knowledge required. No topics had an average ranking below a 2; no topics were mostly ranked between no-knowledge and minimal knowledge. This means that the survey participants believe the topics provided are all relevant for senior leaders as required knowledge.

The average table provides us with another data form to analyze against the best merge table. C37-Cyber security framework was ranked at an 80 minimal but 20 advanced but in the average table we can see the average is 2.4, given the lowest average was 2.2 and the average 2.7, we can conclude that it was ranked on the lower side however not being the lowest. Given both the low scores for the survey results but the high incidence rate in the literature, this topic can be assumed to be of importance for senior leaders to have a general awareness of, or minimal knowledge.

C39-Cyber security training is displayed on the best merge table as mostly grouped on the minimal category but its average of 2.8 indicates that participants would require senior leaders to be more knowledgeable on the topic. This is due to the topic receiving a 40 in the advanced category. Its high incidence rate in the literature also suggests this in an important topic.

The average table also helps to support the previous discovery of planning being of greater value than plans themselves. We can see that C32-Disaster recovery planning has a higher average than C29-Disaster recovery plan. The same is repeated in C28-Business continuity planning has a higher average than C27-Business continuity plan. C31-Recovery point objective also has a higher average than C30-Recovery time objective.



An interesting discovery is that C3-vulnerability assessment attained a high average score while cards associated with third party security [C8-Vendor cyber risk profile, C9-Service level agreement, C10-Vendor auditing, C27-Supply chain cyber security] were ranked with a lower average. In fact, C10-Vendor auditing only received a 2.5 while C3-Vulnerability assessment received a 2.9 average. This suggests that participants believe that senior leaders should be more inward-looking and engage more with the organization's internal audits and less with third parties. We can see the same relationship with C11-Risk assessment having a higher average than C8-Vendor cyber risk profile.

The inward-looking approach also seems to only apply to auditing as all three threat categories received an average higher than the total average. C19-Advanced persistent was the card that had the highest rating at 3.2, C18-Types of cyber threats received a 2.9 and C17-Cyber threats received a 2.8. This points towards the participants believing knowledge of threats being of high importance to senior leaders.

We can see an inverse relationship between the threat [C17-18-19] and risk [C11 and C14] group with the security policy [C20-21-22] and cyber insurance [C5-6] groups. C17-Cyber threats received a 2.8 while C19-APT received 3.2 and C18-Types of cyber threats received 2.9. In this group the more general concept (Cyber threats) received a lower average than a more concrete interpretation of the concept, such as APT, or a more specific aspect of a concept, such as Types of cyber threats. We can see the same happening with the Risk group where the more general concept (C14-Risk with 2.8) received a lower average than a more specific aspect of the concept (C11-Risk assessment with 3). The reverse can be seen with the security policy group where C20-Security policies was given a 3 while C21-Types of security policies a 2.8 and C22-Security policy creation a 2.9. In the Cyber insurance group C5-Cyber insurance was given a 3 and C6-Cyber insurance coverage components was given a 2.8. From this we can extrapolate that survey participants don't follow a single mentality of universally giving a higher or lower value to generalized concepts but make the distinction based on the topic. In some cases, the knowledge about the general concept is more important than knowledge of a more concrete application or interpretation of the topic. From the results, we can see that having knowledge of specific threats is more important than generally knowing what a threat is as well as knowing about risk assessment is more important than knowing about the

general concept of risk. In the case of the threat group the more specific the topic was about concrete threats the higher average it received.

The average table also provides us with insight into risk mitigation. The general concept of risk mitigation was included in C15-Risk mitigation strategies. Risk mitigation strategies are avoid, transfer, reduce, and retain. Other than retain, a concrete form of each strategy was provided. C5-Cyber insurance for transfer, even though complete risk avoidance is very rarely possible C33-Backup strategy is aligned with risk avoidance as well as the security policy group(C20-22), C40-Access controls and C41-Access control models for risk reduction. Risk transfer is reliant on business impact, liability, and cost, while avoidance and reduction are more reliant on controls and technical mitigations. As such, we can see the participants assigning more importance to cyber insurance, a risk transfer strategy, than to access controls or backup strategy. Since business impact, liability, and cost are all business decisions we can again see, as was the case with Recovery Point Objective receiving a higher average than Recovery Time Objective, that survey participants place important in senior leaders being involved in the impact aspect of information security.

The topics with the lowest average mainly deal with more technical aspects, as was the case with table 4, we can see that C42-Operational security, C43-Cryptography, C40-Access controls, and C10-Vendor auditing had the lowest averages. This also furthers reinforces the point that participants believe senior leaders should focus on impact and not on the technical aspects.

Topics that mainly concern people, C38-Human resources security, C34-Cybersecurity committee, and C39-Cyber security training all scored around the average. The average being 2.77, C38 has a 2.7, C34 a 2.7 and C39 a 2.8. These three cards cover a topic in which dealing with people is its focus, whether it be training or overseeing a cyber security committee. This indicates that the topics have importance but are not the most critical.

## 8. Conclusions and Future Research

Senior leaders have a great impact in how an organization manages risk, threats, and its mitigation strategies. This study discussed how non-IT senior leaders are becoming a greater threat to organization's information security assets and systems, as such this study aimed to create a list of topics in the realm of information security which senior leaders should have knowledge of. A desk review was performed to derive a list of topics to be presented in a survey given to 10 CISOs, CIOs, and CTOs in which they were asked to categorize each topic into what level of knowledge they believed senior leaders should have. The results of the survey were presented and analyzed.

Each participant was asked to categorize each topic into one of four categories that are on a scale of levels of knowledge. An example of what the different levels of knowledge might mean for a topic was presented to the participants in the survey instructions, participants might have different meanings for what each level of knowledge is for each category. However, since the categories are on a scale, we can gauge the level of importance each participant assigns to the topic by measuring the frequency in which it was categorized in the same group, which was done in the BMM analysis and the overall average score it received, which was done in the summary section.

The initial conclusion from survey is that information security topics which deal with business impact are more important than those dealing with technical aspects. As non-IT senior leaders deal with business decisions, they require knowledge in the business aspect of information security. Having knowledge of risk transfer strategies such as Cyber insurance is valuable as they understand business impact.

Senior leaders require knowledge of the threats their organization faces, especially high impact threats like Advanced Persistent Threats. Cyber threats and types of threats are all topics in which senior leaders should have knowledge of how threats affect their organizations and not simply which threats is the organization at risk of.

We can conclude that the topics dealing with people (Human resources security, cyber security training, cybersecurity committee) and those dealing with third party vendors (SLA, Supply chain security, Vendor risk profile) are of moderate importance.

Information security incidents, incident management, incident response playbook can be concluded are of higher importance than the incident response team and incident response plan. We can again conclude that knowledge about management and planning is more important than knowledge of plans themselves.

Senior leaders' role is oversight as well, security controls and security policies are tools to fulfill their oversight role and as such are important to have knowledge of. It can be concluded that senior leaders should have moderate knowledge into the organization's disaster recovery and business continuity proceedings.

From the survey analysis, it can be concluded that it is more important for senior leaders to have knowledge about the planning more so than the plans themselves. We can see this in both Disaster recovery planning vs. Disaster recovery plan and Business continuity planning vs Business continuity plan. Senior leaders already have knowledge into business impact, as such it is important to provide them with the knowledge of how business impact correlates with information security so that they can participate in planning for incidents and breaches. Non-IT senior leaders make decisions based on business impact, so the knowledge of how impact is measured and used in information security proceedings, as in disaster recovery planning, business continuity planning, risk assessments is important to have.

We can also conclude that the incidence rate from the literature and desk review has little correlation with the ranking provided by the survey. Topics like advanced persistent threat, which received the highest average, also received the lowest incidence rate at 5%. The literature continued to discuss topics of IS asset management at 60% and cyber security framework at 45% but the survey ranked them lower than average. Risk assessment received the highest incidence rate at 85% and it was also ranked on the higher end with an average of 3. This further demonstrates that empirical analysis is needed in this field of study.

Future research could focus on delivering concrete definitions of what each of the levels of knowledge mean for the topics. Future research could also focus on developing training programs which use the list of topics as a basis for its content. Given this study's survey limitations, further research could be done to amplify the survey audience to include more participants to lessen the impact of bias as well as including different types of participants.

Business and IT consultants could be included in future surveys as a neutral party between IT and non-IT senior leaders, using their knowledge of IS operations from an outsider perspective. Non-IT senior leaders could also be included in future surveys in order for them to communicate in which areas of IS do they feel their knowledge is lacking. Surveying these three groups would provide us with a broader understanding of the problem and possible new conclusions could be derived from a broader survey.

## References

- [1] "Cybercrime Report", *Cybersecurity Ventures*, 2017. [Online]. Available: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. [Last Accessed: April 22 2018].
- [2] "iPass-2017 Mobile Security Report", *Ipass.com*, 2017. [Online]. Available: <https://www.ipass.com/wp-content/uploads/2017/05/iPass-2017-Mobile-Security-Report.pdf>. [Last Accessed: April 22 2018].
- [3] CYBERARK, "CYBERARK Survey Finds Executives Overly Reliant on Compliance Metrics to Measure Security Program Effectiveness", 2015. Available: <https://www.cyberark.com/press/cyberark-survey-finds-executives-overly-reliant-on-compliance-metrics-to-measure-security-program-effectiveness/>. [Last Accessed: April 22 2018].
- [4] M. Beasley, B. Branson, B. Hancock, "The State of Risk Oversight: An Overview of Enterprise Risk Management Practices", *ERM at Poole College of Management, North Carolina State University*, 8<sup>th</sup> Edition, March 2017. [Online]. Available: [https://erm.ncsu.edu/az/erm/i/chan/library/AICPA\\_ERM\\_INITIATIVE\\_Research\\_Study\\_2017.pdf](https://erm.ncsu.edu/az/erm/i/chan/library/AICPA_ERM_INITIATIVE_Research_Study_2017.pdf) [Last Accessed: April 22 2018]
- [5] "What Every CEO Should Understand About Security", 2016, [Online]. Available: <https://noahitservices.com/wp-content/uploads/WP-What-Every-CEO-Should-Understand-About-Security.pdf> [Last Accessed: April 22 2018]
- [6] F. Spidalieri, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat", Pell Center for International Relations and Public Policy 2013, pg. 2. [Online]. Available: [http://www.salve.edu/sites/default/files/filesfield/documents/pell\\_center\\_one\\_leader\\_time\\_13.pdf](http://www.salve.edu/sites/default/files/filesfield/documents/pell_center_one_leader_time_13.pdf) [Last Accessed: April 22 2018]
- [7] "What Every CEO Needs to Know About Cybersecurity", *AT&T Cybersecurity Insights Vol 1*. [Online]. Available: <https://www.business.att.com/cybersecurity/docs/decodingtheadversary.pdf> [Last Accessed: April 22 2018]
- [8] "The CEO's Guide to Navigating the Threat Landscape", *AT&T Cybersecurity Insights Vol 4*. [Online]. Available: <https://www.business.att.com/cybersecurity/docs/vol4-threatlandscape.pdf> [Last Accessed: April 22 2018]
- [9] "(ISC)2 Information Security Certifications", *(ISC)²*. [Online]. Available: <https://www.isc2.org/Certifications> [Last Accessed: April 22 2018]
- [10] "CompTIA Security+", *CompTIA*. [Online]. Available: <https://certification.comptia.org/certifications/security> [Last Accessed: April 22 2018]
- [11] "Certified Information Security Manager (CISM)", *ISACA*. [Online] Available: <http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx> [Last Accessed: April 22 2018]
- [12] "CGEIT Certified in the Governance of Enterprise IT: Job Practice Areas", *ISACA*. [Online]. Available: <https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Job-Practice-Areas/Pages/default.aspx> [Last Accessed: April 22 2018]

- [13] “The CISSP CBK Domains: Information and Updates”, *Infosec Institute*. [Online]. Available: <http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/> [Last Accessed: April 22 2018]
- [14] D. Shoemaker, W.A. Conklin, *Cybersecurity: The Essential Body Of Knowledge*, USA, Cengage Learning, 2011, pp. 67-75
- [15] BDO Global, “CFOs are now also cybersecurity custodians”, 2017. [Online]. Available: <https://www.bdo.global/en-gb/insights/advisory/cybersecurity/cfo-role-extends-into-cybersecurity> [Last Accessed: April 22 2018]
- [16] D. McCann, “CFOs Can Move the Needle on Cyber-Security”, 2014. [Online]. Available: <http://ww2.cfo.com/risk-management/2014/07/cfos-can-move-needle-cyber-security/> [Last Accessed: April 22 2018]
- [17] J. C. Thomson, “Cybersecurity Requires Foresight”, Institute of Management Accountants 2017. [Online]. Available: <https://www.ifac.org/global-knowledge-gateway/risk-management-internal-control/discussion/cybersecurity-requires> [Last Accessed: April 22 2018]
- [18] A. Reschke, “Today’s #1 Cyber Crime Fighter (It’s Not Who You Think)”, *D!igitalist Magazine* 2015. [Online]. Available: [http://www.digitalistmag.com/cyber\\_security/2015/08/12/todays-1-cyber-crime-fighter-not-think-03265007](http://www.digitalistmag.com/cyber_security/2015/08/12/todays-1-cyber-crime-fighter-not-think-03265007) [Last Accessed: April 22 2018]
- [19] A. Tall, J. Le, J. Sherer, “Increased C-Suite Recognition of Insider Threats Through Modern Technological and Strategic Mechanisms”, *Proceedings of the 15<sup>th</sup> European Conference on Cyber Warfare and Security 2016*, pp. 428-433
- [20] *UCISA Information Security Management Toolkit*, Chapter 8, Universities and Colleges Information Systems Association,
- [21] F. Spidalieri, “One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat”, *Pell Center for International Relations and Public Policy* 2013. [Online]. Available: [http://www.salve.edu/sites/default/files/filesfield/documents/pell\\_center\\_one\\_leader\\_time\\_13.pdf](http://www.salve.edu/sites/default/files/filesfield/documents/pell_center_one_leader_time_13.pdf) [Last Accessed: April 22 2018]
- [22] R. A. Rothrock, J. Kaplan, F. Van Der Oord, “The Board’s Role in Managing Cybersecurity Risks”, *MIT SLOAN MANAGEMENT REVIEW*, Winter 2018
- [23] US Department of Homeland Security, “Cybersecurity Questions for CEOs”. [Online]. Available: <https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf> [Last Accessed: April 22 2018]
- [24] University of Cambridge, “Research: Requirements, Skills, and Knowledge”, 2018. [Online]. Available: <https://www.rdp.cam.ac.uk/camrdf/research-requirements-skills-and-knowledge> [Last Accessed: April 22 2018]
- [25] D. M.S. Lee, E. M. Trauth, D. Farwell, “Critical Skills and Knowledge Requirements of IS Professionals: A Joint Academic/Industry Investigation”, *MIS Quarterly*, Vol. 19, No.3 September 1995, pp. 313-340
- [26] Z. Abedin, E. Biskup, K. Silet, J. Garbutt, K. Kroenke, M. Feldman, R. McGee, M. Fleming, H. A. Pincus, “Deriving Competencies for Mentors of Clinical and

- Translational Scholars”, *Clinical and Translational Science*, Vol.5 No.3,2012, pp. 273-280
- [27] H.T. Ingason, H.I. Jonasson, “Contemporary knowledge and skill requirements in project management”, *Project Management Journal*, Vol. 40, No. 2, pp. 59-69
- [28] Information technology – Security techniques – Information security management systems- Requirements, ISO/IEC 27001 2013 Annex A
- [29] A. Nawaz, “A Comparison of Card-sorting Analysis Methods”, *Proceedings of the 10<sup>th</sup> Asia Pacific Conference on Computer-Human Interaction*, 2012, pp. 583-592
- [30] E.F. Cataldo, R.M. Johnson, L. A. Kellstedt, L.W. Milbrath, “Card Sorting as a Technique for Survey Interviewing”, *Public Opinion Quarterly*, Vol. 34, No. 2, Jan 1970, pp. 202-215
- [31] N. Nurmuliani, D. Zowghi, S. P. Williams, “Using Card Sorting Technique to Classify Requirements Change”, *Proceedings of the 12<sup>th</sup> IEEE International Requirements Engineering Conference*, 2004
- [32] Y. Wang, Y. Sure, R. Stevens, A. Rector, “Knowledge Elicitation Plug-in for Protégé: Card Sorting and Laddering”, Institute AIFB, University of Karlsruhe, Germany 2006. [Online]. Available: <http://www.neon-project.org/web-content/images/Publications/knowledge%20elicitation%20plugin%20for%20protege%20-%20card%20sorting%20and%20laddering.pdf> [Last Accessed: April 22 2018]
- [33] European Commission, “What is an SME?” 2018. [Online]. Available: [http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition\\_et](http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_et) [Last Accessed: April 22 2018]
- [34] Fitzgerald T., “Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other”, Taylor&Francis Group, [Online]. Available: <https://pdfs.semanticscholar.org/94e0/7446a534e1cba8e831b94489bdbcbe3f24ae.pdf> [Last Accessed: May 7 2018]
- [35] A. Tang, “A guide to penetration testing”, *Network Security* Vol 2014, No. 8 pp. 8-11
- [36] R. Stevens, “Calcifying Crisis Readiness”, *LISA 17* 2017. [Online]. Available: <https://www.usenix.org/conference/lisa17/conference-program/presentation/stevens> [Last Accessed: April 22 2018]
- [37] J. Yeo, “Using penetration testing to enhance your company’s security”, *Computer Fraud & Security* Vol. 2013 No.4 April 2013, pp. 17-20
- [38] Contingency Planning Guide for Federal Information Systems, NIST Special Publication 800-34 Rev.1 May 2010, National Institute of Standards and Technology
- [39] AT&T, “The CEO’s Guide to Cyberbreach Response”, *AT&T Cybersecurity Insights* Vol 3. [Online] Available:<https://www.business.att.com/cybersecurity/docs/cyberbreachresponse.pdf> [Last Accessed: April 22 2018]
- [40] S. K. Ishaq, “Cyberinsurance Value Generator or Cost Burden”, *ISACA Journal*, Vol 5 2016. [Online] Available: <https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberinsurance-value-generator-or-cost-burden.aspx> [Last Accessed: April 22 2018]



- [41] M. Singh, A.P. Arora, "Perspective and Growth of Cyber Insurance" *World Journal of Research and Review*, Vol 4, No. 6, June 2017, pp. 61-64
- [42] A. Matney and B. Fannin, "The Challenges of Third-Party Data Protection", *Risk Management Magazine*, 2014. [Online]. Available: <http://www.rmmagazine.com/2014/12/02/the-challenges-of-third-party-data-protection/>. [Last Accessed: April 22 2018]
- [43] D. Wu and D. Olson, "Enterprise risk management: a DEA VaR approach in vendor selection", *International Journal of Production Research*, vol. 48, no. 16, pp. 4919-4932, 2010
- [44] P. Patel, A. Ranabahu and A. Sheth, "Service Level Agreement in Cloud Computing", Kno.e.sis Publications, 2009. Available: <http://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=1077&context=knoesis>. [Last Accessed: April 22 2018]
- [45] M. Butkovic, "Cyber SLAs: Practice and Limitations in "Outsourcing Risk"", 2015. Available: [https://resources.sei.cmu.edu/asset\\_files/Podcast/2015\\_016\\_001\\_435531.pdf](https://resources.sei.cmu.edu/asset_files/Podcast/2015_016_001_435531.pdf). [Last Accessed: April 22 2018]
- [46] ISACA, "G4 Outsourcing of IS Activities to other Organizations", ISACA, 2008. Available: <https://csbweb01.uncw.edu/people/ivancevichd/classes/MSA%20516/Extra%20Readings%20on%20Topics/Outsourcing/ISACA%20Audit%20Guideline%20Outsourcing.pdf> [Last Accessed: April 22 2018]
- [47] Cooperative Systems, "What every CEO should understand about security", 2015. [Online]. Available: <https://noahitservices.com/wp-content/uploads/WP-What-Every-CEO-Should-Understand-About-Security.pdf> [Last Accessed: April 22 2018]
- [48] L. Fouche, "Managing risk with cyber insurance", BDO Global, September 2017. [Online]. Available: <https://www.bdo.global/en-gb/insights/advisory/cybersecurity/cyber-insurance-managing-the-risk> [Last Accessed: April 22 2018]
- [49] Infosec Institute, "CIA Triad", November 2016. [Online]. Available: <http://resources.infosecinstitute.com/cia-triad/#gref> [Last Accessed: April 22 2018]
- [50] Information technology – Security Techniques – Information security risk management, ISO/IEC 27005:2011
- [51] S. Ritchie, "Security Risk Managements", *ISACA Atlanta Chapter, Geek Week*, August 2013. [Online]. Available: <https://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Security%20Risk%20Management.pdf> [Last Accessed: April 22 2018]
- [52] Information technology – Security techniques – Information security risk management, BS ISO/IEC 27005:2008
- [53] M. Jouini, L.B.A. Rabai, A. B. Aissa, "Classification of Security Threats in Information Systems", *Procedia Computer Science*, Vol. 32, 2014, pp. 489-496
- [54] ISACA, "2015 Advanced Persistent Threat Awareness – Third Annual", 2015. [Online]. Available: [http://www.isaca.org/Knowledge-Center/Research/Documents/2015-advanced-persistent-threat-awareness\\_whp\\_eng\\_1015.pdf?regnum=423221](http://www.isaca.org/Knowledge-Center/Research/Documents/2015-advanced-persistent-threat-awareness_whp_eng_1015.pdf?regnum=423221) [Last Accessed: April 22 2018]

- [55] A. Shulman, “What CEOs should know about advanced persistent threats and industrialized hacking”, *SC Magazine*, 2010. [Online]. Available: <https://www.scmagazine.com/what-ceos-should-know-about-advanced-persistent-threats-and-industrialized-hacking/article/557653/> [Last Accessed: April 22 2018]
- [56] AT&T, “What Every CEO Needs to Know About Cybersecurity”, *AT&T Cybersecurity Insights*, Vol. 1. [Online]. Available: <https://www.business.att.com/cybersecurity/docs/decodingtheadversary.pdf> [Last Accessed: April 22 2018]
- [57] Diligent, “Five Best Practices for Information Security Governance”, 2016. [Online]. Available: [http://diligent.com/wp-content/uploads/2016/10/WP0018\\_UK\\_Five-Best-Practices-for-Information-Security-Governance.pdf](http://diligent.com/wp-content/uploads/2016/10/WP0018_UK_Five-Best-Practices-for-Information-Security-Governance.pdf) [Last Accessed: April 22 2018]
- [58] H. F. Tipton, M. Krause, *Information Security Management Handbook*, Fifth Edition, pp. 921-924
- [59] P. Clawson, “7 Things Every CEO Should Know About Information Security”, Lumesion Security 2011. [Online]. Available: <https://www.slideshare.net/HeuvelMarketing/7-things-every-ceo-should-know-about-information-security-7303085> [Last Accessed: April 22 2018]
- [60] AT&T, “The CEO’s Guide to Cyberbreach Response”, *AT&T Cybersecurity Insights*, Vol. 3. [Online]. Available: <https://www.business.att.com/cybersecurity/docs/cyberbreachresponse.pdf> [Last Accessed: April 22 2018]
- [61] K. Pritchett, “The importance of Cyber Incident Response Plans and How to Create Them”, *Elon Business Law Journal*, June 2017. [Online]. Available: <http://blogs.elon.edu/blj/2017/06/30/the-importance-of-cyber-incident-response-plans-and-how-to-create-them/> [Last Accessed: April 22 2018]
- [62] T. Bandos, “Building Your Incident Response Team: Key Roles and Responsibilities”, *Digital Guardian*, Field Guide to Incident Response 2017. [Online]. Available: <https://digitalguardian.com/blog/building-your-incident-response-team-key-roles-and-responsibilities> [Last Accessed: April 22 2018]
- [63] V. Cerullo, M.J. Cerullo, “Business Continuity Planning: A Comprehensive Approach”, *Information Systems Management*, Vol. 21 No. 3, pp 70-78
- [64] M. Gregg, “Business Continuity and Disaster Recovery Planning” 2009. [Online]. Available: <http://www.pearsonitcertification.com/articles/article.aspx?p=1329710&seqNum=3> [Last Accessed: April 22 2018]
- [65] Contingency Planning Guide for Federal Information Systems, NIST 800-34 Rev 1, National Institute of Standards and Technology
- [66] O. Alhazmi, Y. Malaiya, “Assessing Disaster Recovery Alternatives: On-Site, Colocation or Cloud”, *2012 IEEE 23<sup>rd</sup> International Symposium on Software Reliability Engineering Workshops*.

- [67] J. Singh, “Understanding RPO and RTO”, Druva 2008. [Online]. Available: <https://www.druva.com/blog/understanding-rpo-and-rto/> [Last Accessed: April 22 2018]
- [68] S. M. Landefeld, L. R. Mejia, A. C. Handy, “Board Tools for Oversight of Cybersecurity Risk”, *Corporate Governance Advisor*, Vol. 23 No.3, June 2015, pp. 1-9
- [69] Microsoft, “Microsoft Security Development Lifecycle”. [Online]. Available: <https://www.microsoft.com/en-us/sdl/default.aspx> [Last Accessed: April 22 2018]
- [70] H. Misra, *Information Systems Management in Business and Development Organizations*, PHI, October 2013, pp. 361-365
- [71] Boisvert R., “What every CEO needs to know about cybersecurity: A background paper”, I-SEC Integrated Strategies, 2014 [Online]. Available: <http://www.ceocouncil.ca/wp-content/uploads/2014/04/What-Every-CEO-Must-Know-Cyber-April-4-2014-Final.pdf> [Last Accessed: May 7 2018]

## Appendix 1 – Sources for Desk Review

- [1] Diligent, “Five Best Practices for Information Security Governance”, 2016, [Online]. Available: [http://diligent.com/wp-content/uploads/2016/10/WP0018\\_UK\\_Five-Best-Practices-for-Information-Security-Governance.pdf](http://diligent.com/wp-content/uploads/2016/10/WP0018_UK_Five-Best-Practices-for-Information-Security-Governance.pdf) [Last Accessed: May 7 2018]
- [2] “What Every CEO Should Understand About Security”, 2016, [Online]. Available: <https://noahitservices.com/wp-content/uploads/WP-What-Every-CEO-Should-Understand-About-Security.pdf> [Last Accessed: April 22 2018]
- [3] Saint-Germain, R., “Information Security Management Best Practice Based on ISO/IEC 17799”, *Information Management Journal* Vol. 39 No. 4, pp 60-62, 64-66.
- [4] AT&T, “What Every CEO Needs to Know About Cybersecurity”, AT&T Cybersecurity Insights Vol. 1, [Online]. Available: <https://www.business.att.com/cybersecurity/docs/decodingtheadversary.pdf> [Last Accessed: May 7 2018]
- [5] Thomson, J.C., “Cybersecurity Requires Foresight”, IFAC, Risk Management & Internal Control, April 2017, [Online]. Available: <https://www.ifac.org/global-knowledge-gateway/risk-management-internal-control/discussion/cybersecurity-requires> [Last Accessed: May 7 2018]
- [6] Ursillo, S. J., “ Does your Cyber Security Include Governance? It Should”, IFAC, Risk Management & Internal Control, November 2017, [Online]. Available: <https://www.ifac.org/global-knowledge-gateway/risk-management-internal-control/discussion/does-your-cyber-security> [Last Accessed May 7 2018]
- [7] Shoemaker D, Conklin A., *Cybersecurity: The Essential Body of Knowledge*, Cengage Learning, 2011, pp 67-75
- [8] Durbin S, “Data and Dollars: The Role of the CFO in Cybersecurity”, *Connected Futures, Executive Insights by Cisco*, November 2015, [Online]. Available: <https://connectedfutures.cisco.com/article/data-and-dollars-the-role-of-the-cfo-in-cybersecurity/#.WgRMimiCyUk> [Last Accessed: May 7 2018]
- [9] BDO Global, “CFO role extends into Cybersecurity”, September 2017. [Online]. Available: <https://www.bdo.global/en-gb/insights/advisory/cybersecurity/cfo-role-extends-into-cybersecurity> [Last Accessed: May 7 2018]
- [10] Bailey T., Kaplan J., Rezek C., “Why Senior Leaders are the Front Line Against Cyberattacks” McKinsey&Company, June 2014, [Online]. Available: <https://digitalstrategy.nl/files/2014.06-E-Why-senior-leaders-are-the-front-line-against-cyberattacks1.pdf> [Last Accessed: May 7 2018]
- [11] Landefeld S., Mejia L., Handy A., “Board Tools for Oversight of Cybersecurity Risk”, *Corporate Governance advisor*, Vol.23, No.3, June 2015
- [12] North J., Pascoe R., Westgarth C., “Cyber security and resilience – it’s all about governance”, *Governance Directions*, April 2016 pp. 146 – 151

- [13] Boisvert R., “What every CEO needs to know about cybersecurity: A background paper”, I-SEC Integrated Strategies, 2014 [Online]. Available: <http://www.ceocouncil.ca/wp-content/uploads/2014/04/What-Every-CEO-Must-Know-Cyber-April-4-2014-Final.pdf> [Last Accessed: May 7 2018]
- [14] Fitzgerald T., “Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other”, Taylor&Francis Group, [Online]. Available: <https://pdfs.semanticscholar.org/94e0/7446a534e1cba8e831b94489bdbcbe3f24ae.pdf> [Last Accessed: May 7 2018]
- [15] MetricStream, “Top Eight Priorities for Cyber Security and BCM Leaders in 2017”, 2017, [Online]. Available: <https://www.metricstream.com/insights/Cyber-Security-and-BCM-priorities.htm> [Last Accessed :May 7 2018]
- [16] US Department of Homeland Security, “Cybersecurity Questions for CEOs” [Online]. Available: [https://www.dhs.gov/sites/default/files/publications/Cybersecurity%20Questions%20for%20CEOs\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/Cybersecurity%20Questions%20for%20CEOs_0.pdf) [Last Accessed: May 7 2018]
- [17] DefenseStorm, “10 Questions every CEO must ask their Cybersecurity team”, October 2015, [Online]. Available: <https://www.bankinfosecurity.com/whitepapers/10-questions-every-ceo-must-ask-their-cybersecurity-team-w-1945> [Last Accessed: May 7 2018]
- [18] Rothrock R., Kaplan J., Van der Oord F., “The Board’s Role in Managing Cybersecurity Risks”, *MIT Sloan Management Review*, Vol.50 No.2, Winter 2018, pp 12 – 17
- [19] Sweeny B., “Cybersecurity is Every Executive’s Job”, *Harvard Business Review*, September 2016, [Online]. Available: <https://hbr.org/2016/09/cybersecurity-is-every-executives-job> [Last Accessed: May 7 2018]
- [20] Williams P., “Executive and board roles in information security”, *Network Security*, Vol. 2007 No.8. pp 11-14