A Work Project, presented as part of the requirements for the Award of a Masters

Degree in Finance from Nova School of Business and Economics

CYBERSECURITY: Perspectives from Banking & Capital Markets, Insurance and Wealth & Asset Management sectors.

Ana Rita Gomes Chaves Fernandes

#3305

of:

Professor Emanuel Gomes

Ricardo André, Assurance Partner at EY

January 2018

Abstract:

This study focus on the perspective of cybersecurity in the financial services industry namely the Banking & Capital Markets, Insurance and Wealth & Asset Management sectors. Suffering the highest costs of cybersecurity and dealing with increasing sophisticated attacks, organizations within this industry must consider cyberattacks in their strategic planning.

The comparison analysis suggests that the main vulnerability appointed by the three sectors are careless employees, their lack of training as well budget constraints and minor executive support. Moreover, the Board should acknowledge itself about information security in order to establish effective preventive and reactive measures. At last, cyber insurance interest is improving within the three sectors.

Keywords: Cybersecurity; Financial services; Careless Employees; Cybersecurity Budget.

1. Introduction

Today's technological world is impacting businesses, people's lives and the way cybersecurity evolves (OECD, 2017). In the past decades, technologies have been facing a tremendous growth so as the relevance of information security. A large-scale breach of cybersecurity was included in the top five of the most serious risks facing the world today by the World Economic Forum (2017). Furthermore, according to Cybersecurity Ventures (2017), over the next five years, global spending on cybersecurity will exceed $ 1 trillion cumulatively. The permanent mobile connectivity and the exponential growth of computing power boosted the development and innovation in many sectors, however, it increased their exposure to cyberattacks. Sophistication on these attacks allowed cybercriminals to exploit vulnerabilities of many organizations and governments (Walls, 2014) (See **Appendix 2.1-2.3**). By 2021, cybersecurity damages are expected to double, costing the world approximately 6€ trillion annually (Cybersecurity Ventures, 2017). Although these cyberattacks have damaged various industries already, the financial services sector is the one that suffers more harm. Indeed, according to Europol (2017), it is the sector with the highest cost of cybercrime.

There are some studies about cybersecurity concepts and ways to protect and expand awareness (Craigen, Diakun-Thibault and Purse, 2014; Fernandes, 2013; Porche, Sollinger and McKay, 2011), as well as a systematic review of literature regarding cyber situational awareness (Franke and Brynielsson, 2014). However, there are some gaps in understanding organizations' vulnerabilities in the technological society which should be addressed. Moreover, a perspective of financial services regarding cybersecurity and an explanation of the hiring gap was given, e.g how organizations should hire and retain a cybersecurity professionals (Pierce, 2016). The relevance of insurance coverage to protect

from liability losses is also very discussed (Zureich and William Graebe, 2015). Some articles regarding cyberwar and cyberterrorism are increasing their expression in the literature as well as cybersecurity's governance (Amaral, 2014; Singer and Friedman, 2013; Perez, 2010; Chang and Grabsky, 2017).

The aim of this paper is to perform a comparative analysis regarding cybersecurity awareness within the financial industry, by understanding how the Banking & Capital Markets, Insurance and Wealth & Asset Management sectors have been dealing with the recent evolution of cyberattacks and how budget decisions evolved. Moreover, this study will extend the analysis of the cybersecurity topic mentioning some of the main threats and vulnerabilities encountered by these organizations.

The rest of the paper is structured as follows: first, it reviews the extant literature relevant to cybersecurity and its consciousness within organizations. The second section explains the methodology adopted and presents a brief explanation of the data used in this research. Next, an analysis of the results is presented and discussed. The last section concludes on the topic.

3. Literature Review

In May of 2017, all continents and thousands of enterprises were affected by the *WannaCry* hack, a cyberattack based on ransomware. It was required a payment of redemptions to unlock the affected systems. The attack affected initially telecommunications companies spreading subsequently to energy firms, financial institutions and paralyzing the National Health System in the UK which compromised the normal flow of the economy and society in that period (Petit, 2017; Hern, 2017). The countries affected were Portugal, Russia, Spain, UK, Japan, among others. The most common attacks occurring are based on ransomware, phishing via e-mail and the zero-

days attacks. The latter shuts down every system infected while the first two are easily expanded through e-mail accounts and social networks. According to the "Cost of Cyber Crime Study" information theft remains the most expensive consequence of a cybercrime (Europol, 2017). Many attacks are successful simply because people click on a button disregarding the content or the potential threat. Increasing awareness for cyberattacks is preventing their success (Cybersecurity Ventures, 2017). Human performance was considered the key to the success of development and operation of cybersecurity processes (Boyce et al. 2011). However, Robert Herjavec, founder and CEO at Herjavec Group, stated that employees tend to be the weakest link in an organization. In fact, employees put their organization vulnerable by not being aware of the risks. According to the Global Risks Report, teaching employees to identify, defend and react to "*cyberattacks is the most underspent sector of the cybersecurity industry"* (World Economic Forum, 2017). Actually, in 2014 the global spending on security awareness training for employees was $1 billion. For 2027, this expenditure is expected to reach $10 billion (Cybersecurity Ventures, 2017).

As cybersecurity becomes more relevant, the market labor for this sector suffer some changes. Although some authors defend that the shortage on cybersecurity professionals has been solved throughout the years due to the efforts in education awareness and the arising of new job classifications (Libicki, Senty and Pollak, 2014), it is still an issue affecting organizations which are suffering losses due to this skill gap. In fact, there are, at least, thousands of cyber-related jobs openings due to lack of skilled candidates (Pierce, 2016). Additionally, it is noted the need for more women within cybersecurity industry as only 11% of cybersecurity positions belong to them, according to the Women's Society of Cyberjutsu (Miller, 2017). John Reed Stark, former Chief of the SEC's Office of Internet Enforcement, emphasized the cybersecurity labor issue, once he considers the

greatest threat not to be *state-sponsored cyberattacks*, but *the severe cybersecurity labor shortage which is* expected to reach 1.5 million job openings by 2019.

In the beginning of this decade, Chang (2012) debated about cybersecurity's interdisciplinary nature *"(...) Humans must defend machines that are attacked by other humans using machines (...)".* Two years later Craigen, Diakeun-Thiab and Purse (2014) developed a compilation of all the available literature regarding cybersecurity with the purpose of achieving a concise and inclusive definition: "*Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure form de facto property rights"* (p.13). In order to better understand the term "*Cybersecurity"* a partition was made to clearly define each component: *Cyber* and *Security.* According to Oxford (2014), *"Cyber"* refers to electronic communications networks and the virtual reality. Wiener (1948) had already developed the term "*cybernetics"* and Gibson's (1984) enhanced and popularized the term "cyberspace". The year before, Public Safety Canada (2010) provided a definition of cyberspace "*the electronic world created by interconnected networks of information technology and the information on those networks"* which was complemented by Deibert & Rohozinski (2010) who stated that it is a dynamic and multilevel system that represent human intentions. Baldwin (1997) suggested the reformulations of each individual' conceptions of security "*as clearly and precisely as possible*". Furthermore, Oxford (2014) concluded that the principal presumption of security is to be safe from potential threats or dangers.

Recently, the literature was enriched with an heuristic model for cybersecurity to depict the challenges organizations face to minimize the costs resulted from insecurity evolving cyberspace (Libicki, Ablon, & Webb, 2015). By creating a framework for how cybersecurity choices are established within an organization, the authors studied variables

such as size, diligence, use of tools and training. They concluded that both training and use of tools increase as a function of size of the organization and value at risk. The diligence factor turns out to be insensitive to these factors given that high-diligence organizations typically obtain greater value on the first tools acquired so that the potential losses to a cyberattack fall rapidly.

There is a consensus that cybersecurity and issues involving cyber threats are evolving with no turning back. Despite the fact that Rid (2011) considers the conflicts in the cyber domain permanent, he states that none pure cyberwar will exist because that will never be sufficient to win on its own. The same applies in the case of a field war as "*No battle will be won without the cyberspace*". Governments have been tightened regulations and adopted cyber security strategies. Among others, we can observe as an example the Government of Canada, the National Information Security Center from Japan and The Federation Council from Russia. The regulations differ from each other (Giles and Hagestad, 2013) but have significant priorities in common such as developing their situational awareness. Furthermore, European Commission created the General Data Protection Regulation (GDPR) which establish rules to ensure information security, namely, personal data. Companies not complying with the rules will be fined up to 20 million euros or 4% of their annual revenue (The European Parliament, 2016). Several recommendations are given for enterprises in order to prepare them to the new regulation such as preparation for data breaches, a special aware for cross-border data transfers as well as organizations' transparent practices (Allen & Overy, 2017). Recognizing cybersecurity as a potential concerning issue at a national level, Fernandes (2013) predicted that an adaptation of GNR *(Guarda Nacional Republicana/* Republican National Guard*)* to the new reality would be crucial following six goals, namely the development, standardization and certification, training and awareness, incident alert and

response, combating cybercrime and critical infrastructure protection. Additionally, the author recommended the development of "Special Police Programs" related to Cyber-Policing in order to raise awareness among citizens and public-private sectors as well as to teach how to recover from a disaster and to keep a resilient business.

The increasing difficulty of defending cyberspace was documented by Porche, Sollinger and McKay (2011) who attributed several causes such as the absence of virtual cyber boundaries, the need of transition between private and public networks, either at a national level or abroad and the fact that cyberspace became a “global commons” which is open to everyone.

By performing a systematic review of the literature on cybersecurity situational awareness, Franke and Brynielsson (2014) identified that more research could be devoted on information exchange as they consider it a driver to expand cyber situational awareness an important for national strategies. Additionally, Hennin (2008) suggested a model for information exchange regarding suspicious IP addresses and two years later, Klump and Kwiatkowski (2010) recommended a model for information exchange about incidents in the power system.

4. Methodology and Data

For the aim of this paper, the author performed a comparison of results of the Global Information Security Survey (GISS) launched by EY Global within 3 sectors: Banking & Capital Markets, Insurance and Wealth & Asset Management sectors. The main goal is to depict trends of cybersecurity awareness within these sectors and understand how evolution of cyberattacks is associated to an increase concern with information security.

Since the data considered for this analysis was obtained from the latest edition of GISS, it should be classified as secondary data. The data collected consists on the results of a

questionnaire launched at a global scale in 2017 which was taken by multiple companies from different sectors all over the world. The choice to perform the study using data that was already collected was mainly due to feasibility issues. It would be extremely difficult to collect data in the same conditions as the authors of the survey did since EY is present in more than 150 countries and has multiple contacts with clients. This year research occurred between June and September of 2017 and included around 1200 respondents from 72 countries. They are typically information security and IT executive or managers and C- level executives. The majority of respondents come from EMEIA (Europe, Middle East, India and Africa) and Americas. There is a diversity of sectors covered by this survey. As one can observe on the **figure 1**, respondents are coming from firms related to Oil & Gas, Telecommunications, Technology, Banking among others.

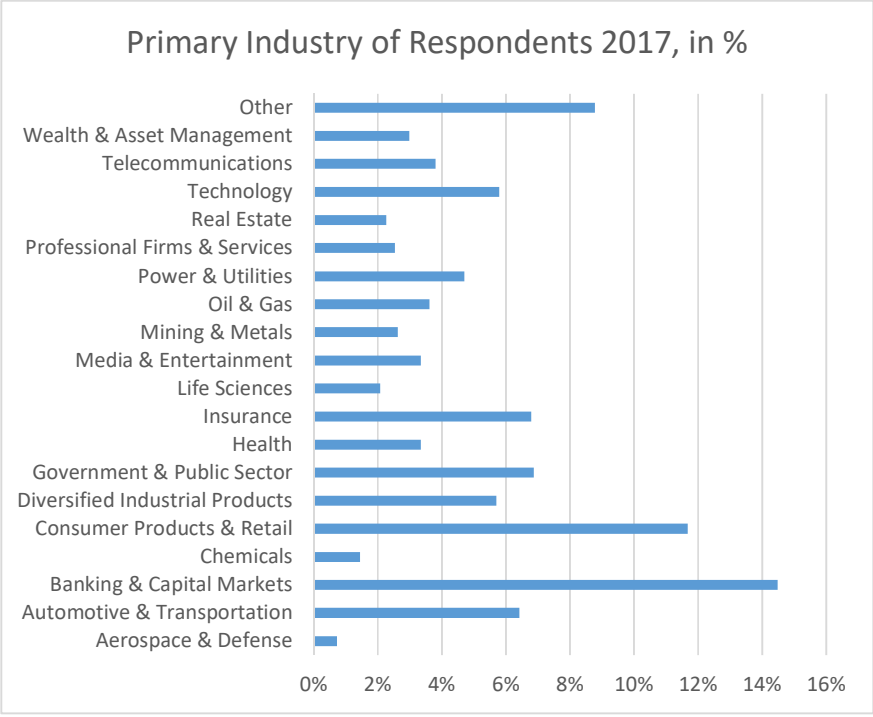


Figure 1 – Primary Industry of Respondents Source (GISS 17-18)

In order to develop a more industry specified comparison, the author of the study decided to strict the sample to a maximum of 3 sectors. Firstly, the author verified that the majority

of the respondents belonged to Banking & Capital Markets, Consumer Products & Retail, Wealth & Asset Management and Insurance (**Figure 1**). Given the relevance that cybersecurity has in Banking & Capital Markets sector, the Insurance one and the Wealth & Asset Management industry and the fact that these sectors suffer the greatest costs concerning information security (Europol, 2017), the analysis of comparison focused on them.

As a result, the sample of this study comprises responses from the sectors mentioned above, totalizing 268 respondents: 160 from Banking & Capital Markets, 75 from Insurance and 33 from Wealth & Asset Management sector. It was not possible to depict all respondents by gender and age range.

The author performed a descriptive analysis of the sample using some statistic methods such as identifying the mode and calculating the arithmetic mean within intervals as the formula below:

$$\bar{X} = \frac{\sum(Xa * Xm)}{\sum(Xa)} \quad (1)$$

Where *Xa* is the absolute frequency and *Xm* is the midpoint of the specific class of interval.

The GISS survey is performed every year to assess the awareness that companies have regarding cybersecurity and their efforts to make their organization more resilient to face cyberattacks. The 20th edition of this questionnaire have 5 sections where a different topic is developed in each section. The first section is a mere description of the organization's profile. The second section concerns strategy, innovation and growth and the following one is about risk. Then, questions relate to technology, people and organization. In the final section, finance and legal topics are approached. In general, the questionnaire relates

to the security budget and investments of the organization, security effectiveness and risks, among others (See **Section A, Appendix 1**).

As an example, the last survey asked respondents "*What is your organization's total annual spend on cybersecurity in US$?*" and to identify variation from last 12 months of the *organization's total security budget* as well as the change expected for the next 12 months. Regarding risk, the survey provide respondents with a list of different type of information and asked them to classify all which they "*believe to be the most valuable to cyber criminals".* Possible options are customer personal and passwords, R&D information, company financial data, information exchanged during M&A activities among others.

5. Presentation and Discussion of Results

Through an analysis of respondent results, it was possible to compare each sector points of view in various topics: past and future variations on cybersecurity budget, additional funding needed to protect the company, main threats and vulnerabilities identified, among others. As mentioned before, three sectors were considered for this analysis: Banking & Capital Markets, Insurance and Wealth & Asset Management.

In order to understand the importance organizations from these sectors give to cybersecurity issues, an analysis on organization's total annual spend on cybersecurity was performed. The latter includes all costs related to process, technology and people. Having these in mind, it was observed that approximately 24% of respondents from the Banking and Capital Markets (BCM) sector spend annually between $1 and $2 million on cybersecurity. Organization's annual expenditures rise up to $50 million for approximately 21% of respondents. On average, organizations' total annual spend on

information security in the Banking and Capital Markets **(BCM)** sector is approximately $12.9 million, including technology, people and process costs.

Roughly one half of respondents from Insurance sector admitted that their organizations' total annual spend on information security was less than 2$ million. It was observed that, on average, organizations' total annual spend on information security in the Insurance sector is approximately $11.9 million. Approximately 28% of organizations in Wealth and Asset Management (WAM) sector are spending, per year, between $1million and $2 million on cybersecurity. On average, cybersecurity' annual spent in the WAM sector is approximately $4.75 million.

Aiming to evaluate the variation of organization's total budget in cybersecurity matters and how cybersecurity is associated with budget's decisions, respondents had to define an interval that reflected the variation of cybersecurity's budget compared to the last 12 months. For the Banking sector, institutions faced, on average, an increase on their organizations' total cybersecurity budget over the last 12 months of approximately 10%. Indeed, approximately 33% of respondents said that cybersecurity budget increased up to 25%. However, 1% of respondents admitted having decreased their cybersecurity budget in the last 12 months.

Nearly a quarter of Insurance respondents admitted an increase up to 25% on their organization's total cybersecurity budget during the last 12 months. Approximately one third of organizations kept the same level on the cybersecurity budget. As a result, on average, insurance sector faced an increase on their organizations' total cybersecurity budget over the last 12 months of approximately 7%.

In the previous year, approximately 40% of organizations from **WAM** sector faced a decrease up to 25% on total cybersecurity budget. Only 3% of organizations expect a

negative variation between 15% and 25% on cybersecurity budget. Overall, on average, wealth management companies faced a decrease on their organizations' total cybersecurity budget over the last 12 months of approximately 7%.

Moreover, respondents delimited an interval that reflected the variation in organization's total cybersecurity budget for the following 12 months. Expectations for this period revealed an increased awareness of impacts and costs cybersecurity can impose to organizations mainly for the banking and insurance sectors. For the first sector, approximately 42% of respondents plan to increase their organization's total cybersecurity budget between 5% and 15%, while approximately 25% admitted to increase it up to 25%. Only 3% considered an increase greater than 25% and almost one third expected no variation in the cybersecurity budget. We can conclude that, on average, financial institutions expect an increase of approximately 9% on their organizations' total cybersecurity budget in the following 12 months. Regarding the Insurance sector, approximately 55% of organizations plan to increase their total cybersecurity budget up to 25% in the next 12 months. Only 2% of respondents admitted to decrease their budget in more than 25%. On average, insurance companies expect an increase of approximately 11% on their organizations' total cybersecurity budget in the following 12 months. Against author expectations, wealth and asset management' organizations are decreasing their attention of cybersecurity. In fact, 68% of respondents admitted a decrease on the cybersecurity budget up to 25%, while approximately 18% believed it would stay in the same level. On average, these companies expect a decrease of approximately 12% on their organizations' total cybersecurity budget in the following 12 months.

In fact, one would expect these positive variations in organizations' total cybersecurity budget either from the past 12 months or the next ones to be associated with the increasing concern of cybersecurity issues. One of the reasons is the harm that cyberattacks cause in

organizations, namely in financial services which suffer the highest costs related to cyber (Europol, 2017). Although with less representability, the negative variation on organizations' total cybersecurity budget in WAM sector was not expected neither its intensification in the following 12 months. Indeed, these results corroborate part of the literature once there are increasing concerns with information security and the probability of attack attempts (Accenture, 2016; Cybersecurity Ventures, 2017; Castelli et al, 2017).

A further question regarding how much additional funding organizations would need to protect the company had similar results within the sectors in analysis. Firstly, approximately 73% of respondents from Banking & Capital Markets sector believe their organization would need up to 25% of additional funding to protect the company and to be aligned with management risk tolerance while 14% consider that 50% of additional funding would be enough to protect the company. On average, institutions within banking and capital markets sector would need approximately 24% of additional funding to be aligned with management's risk tolerance. The result is the same in the insurance sector. Actually, only 5% of respondents admitted needing between 75% and 100% of additional funding to protect the company and to keep in line with management's risk tolerance.

Approximately 80% of wealth and asset management firms believe they would need up to 25% of additional funding in order to protect their companies while only 3% admitted needing between 76% and 100% of additional funding. On average, financial institutions would need approximately 19% of additional funding to be aligned with management's risk tolerance. The **Table nº 2** below summarizes the comparison of average results within the three sectors.

Summary of Cybersecurity's Budget Variation and Additional Funding Needed

(Table 2)

Comparison between sectors	Cybersecuity's Budget Variation		Additional funding needed
	From the last 12 months	For the next 12 months	
Banking & Capital Markets	10,3%	9,4%	24%
Insurance	7%	11%	24%
Wealth & Asset Management	-7%	-12%	19%

An interesting point mentioned before is that **WAM** sector has been decreasing funds in their budget for cybersecurity, however, respondents from this sector consider that they would need, on average, approximately 19% of additional funding to fully protect the company.

There are many threats that may affect organizations, either directly or indirectly. That is one of the main reasons why organizations are increasing their attention in cybersecurity matters. Indeed, these threats may lead to a loss of productivity, damage in organization's reputation and consequently, credibility. In larger scale, if these threats turn into an executed cyberattack, it may affect the normal flow of economic activities, just like the WannaCry attack did, through ransomware (National Audit Office, 2017).

Additionally, phishing attacks are real and most of the times they are successful because employees are not properly trained on how to defend and react in these cases. Most of attacks tempted are successfully done because someone clicks on the button. Therefore, attempts from the literature to enhance the importance of training and preparing employees is consonant with results which suggest that training and raising awareness within organization's employees is crucial to prevent and mitigate these risks (Cybersecurity Ventures, 2017; Libicki, Ablon, & Webb, 2015). Further vulnerabilities identified by organizations and classified as high priority were malware, fraud, outdated information security systems are out-of- date and the use of cloud computing.

In the graphic bellow, one can observe a comparison of the most likely sources of an attack between BCM, Insurance and WAM sectors. Moreover, the graphic includes the overall results which covers all sectors included in this questionnaire.

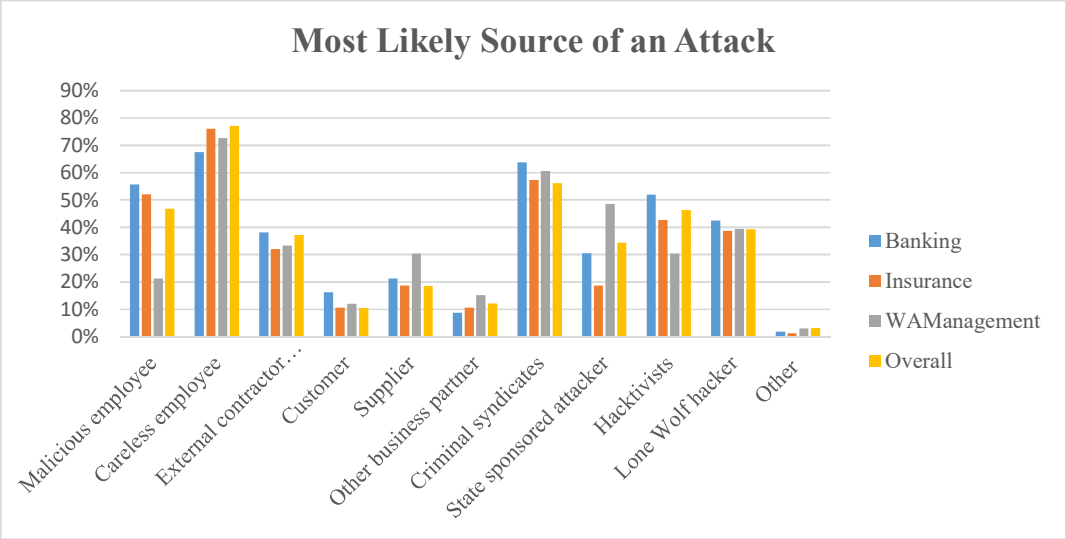


Figure 2 – Most Likely Sources of an Attack

At a first sight, careless employee is considered unanimously the most likely source of an attack. As explained before, training employees and increasing their awareness to potential threats as well as giving good examples and motivating with good practical behaviors is fundamental to decrease the risk organizations face. The second most likely source of an attack, nominated with unanimity are the criminal syndicates. The latter are real and so their revenues. Many criminal syndicates act on the purpose of developing their business either by earning money with stolen data or by creating and selling software. In the second trimester of the current year, an international cybercrime group who designed, developed and sold sophisticated software tools was dismantled due to efforts from Spanish and British law enforcements authorities (Europol, 2017). Other reports' results highlight the increase of incidents attributed to insiders instead of third parties and external hackers. (Castelli et al, 2017).

Hacktivists and Lone Wolf hackers also concerns organizations even though in a smaller scale. State sponsored attacks are more significant for wealth and asset management sector. However, there is a general concern regarding these type of attacks that have been growing in the past years despite some authors undervalued them (Stark and Fontaine 2015). For example, the media insinuate the possibility of the Russians interfering in the last American elections (Lipton et al, 2016) leading to the elaboration of studies on how cyberpower might have interfered. (Intelligence Community Assessment, 2017).

When asked to identify the main challenges that IoT brings to information security, organizations vary too little. They consider that it is harder to know all the assets of the organization, to keep all systems updated in terms of security and to identify suspicious traffic occurring in the network. A further challenge mentioned is the ability to track the access to data within organizations. Moreover, organizations considered that the shortage of skilled resources together with lack of executive support and budget constraints are the main barriers to a broader adoption of IoT devices. Nevertheless, according to Cybersecurity Ventures, IoT will be the main technology driver in 2018.

The top4 priorities regarding information security identified by these sectors are the protection of Intellectual Property, the security of interconnected devices, the automation of robotic process as well as to ensure the security of cryptocurrencies.

It is common on organizations to outsource some information security services. Indeed, according to sector' respondents, the most outsourced information security functions are security monitoring, assessment of vulnerabilities and specific consultancy activities. Further outsourced functions are self-phishing to verify its impact on the organization and one time exercises.

With the purpose of properly protecting the company against cyberattacks, it is crucial that not only employees are trained but also that the Board understand the issue and define a strategy plan according to that scenario.

A Board that is aware of the risks is more prepared to deal with them and to establish effective measures that prevent attacks targeted to organizations. Moreover, as mentioned before, it is important that good practical behavior is encouraged and demonstrated by executives and the Board. As one can observe in **Figure 3,** approximately 40% of respondents recognized that boards have sufficient knowledge of information security to properly evaluate the risks and threats their organization is facing as well as create actions to react. Less than 5% of respondents from the three sectors declared the Board not to have sufficient knowledge on information security with negative consequences on decision-making process. Boards that don't have enough knowledge but are improving their skills are also representative within respondents. As Stark and Fountaine (2015) studied, the cybersecurity topic must receive much attention from boards of directors who should become "actively involved in properly addressing cybersecurity". Furthermore, both authors defend a similar approach as an audit

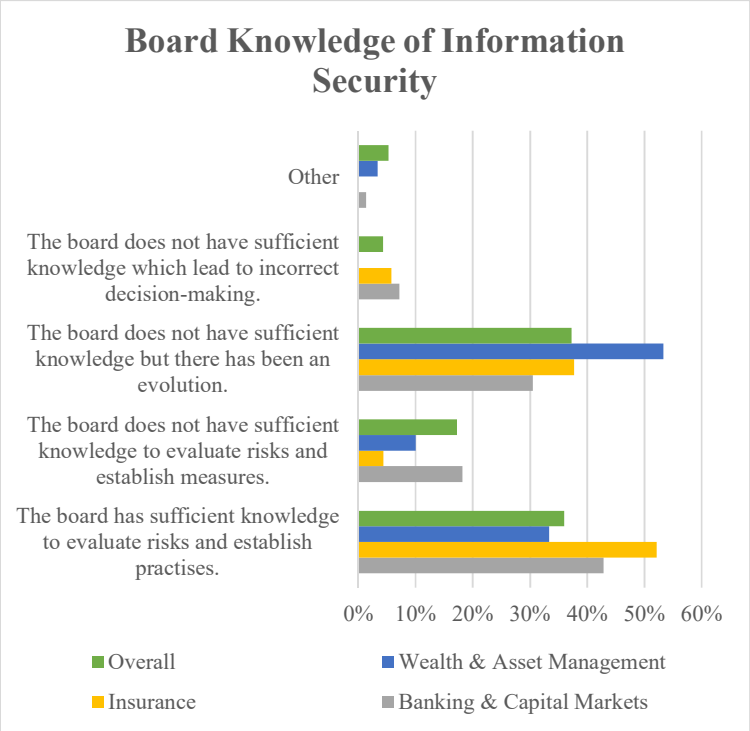


Figure 3 – Board Knowledge of Information Security.

committee for financial statement and reports, characterized by its rigor, skeptically and methodical inquiry.

A high percentage of respondents of the sectors in analysis believe that their organization is likely to detect a sophisticated cyberattack (BCM: 55%, Insurance 41%; WAM 58%). From one fifth to one third of respondents considered unlikely a detection of a sophisticated cyberattack by the company. According to 6-10% of respondents, it is highly unlikely that the organization detect a sophisticated cyberattack (**Appendix 3**).

In the previous year, organizations faced significant cyber breaches that can be attributed to either process or primary controls failures. Outdated systems, insufficient employee awareness exploited via phishing were the most appointed failure. Although with less representability, poorly secured internet-facing systems were determinant to originate significant cyber breaches.

Organizations from the three sectors considered the information security maturity of peer organizations by sector and the effectiveness of technologies more important and useful rather than knowing about the threat intelligence sources effectiveness or allocation of funds in security. In the middle, one can observe that internal reporting structure is also practical but not that relevant for these companies.

As mentioned before, cyberattacks may impact the productivity, raise problems with regulatory institutions and affect reputation of companies. These inevitably influence the revenue of the firm. An estimation of total financial damage related to information security incident over the past year was asked. This estimation covered productivity losses and regulatory fines but excluded costs caused by brand damage. Having these in mind, it was observed that approximately 76% of banking institutions faced a loss between $0 and $100.000 while only 6% suffered a loss greater than $2.5 million. On

average, BAM sector estimation of the total financial damage resulted from information security incidents in the previous year was approximately $253K. In the insurance sector, 78% estimated their financial damages up to $250K and roughly 9% were above $2,5 million. As a result, on average, the predicted financial harm in this sector was approximately $396K. Last but not least, it was verified that nearly two thirds of respondents from wealth and asset management sector faced losses up to $100K and no loss above $500K was estimated over the last year. Consequently, there is an average estimated financial damage on this sector equivalent to, approximately, $117K. Considering the undeniable increasing importance of cybersecurity in these years, organizations must recognize this issue and put in place measures that effectively defend the organization in case of an attack. Not only reacting practices are needed but also preventive ones. On that purpose, respondents from the three sectors were asked to classify their interest in Cyber Insurance. Above, there is **Figure 4** that summarizes the level of interest in cyber insurance within these sectors. In Banking and Capital Markets sector, nearly 28% of respondents confirm to have cyber insurance that meets all requirements and needs of the organization. Around 50% of respondents

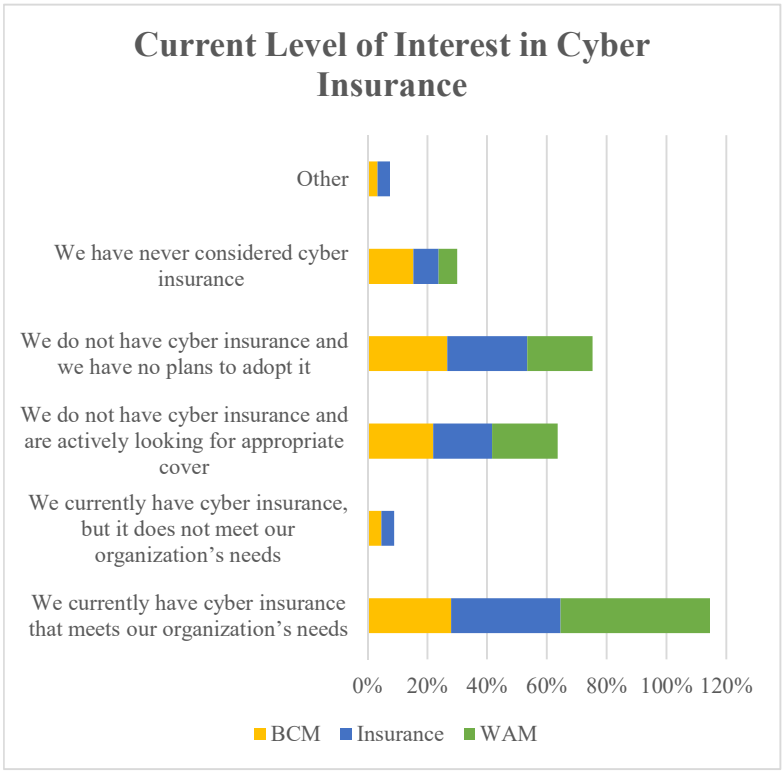


Figure 4 – Current Level of Interest in Cyber Insurance.

don't have any cyber insurance plan from which approximately 27% have no intention to adopt one and the remaining are looking for an effective cover. Actually, 15% of respondents admitted not to even consider a cybersecurity insurance. The path is very similar for both Insurance sector and Wealth & Asset Management sector. The fact that many organizations don't consider the hypothesis of having a cyber insurance is worrisome in the sense that those could suffer damages and they are neither partial nor fully protected with an insurance and, according to Zureich and Graebe (2015), *"A law firm that operates without a specialized cyber liability insurance policy is at risk for significant uncovered exposure in the event of a cyber claim"*.

6. Conclusion

The aim of this research was to analyze perspectives of Banking & Capital Markets, Insurance and Wealth & Asset Management sectors to find how these organizations are facing the rise of cybersecurity importance and which vulnerabilities and threats firms had to deal with. Moreover, this study highlights an important point regarding organizations employees. The results showed that the greatest vulnerability come from either careless or malicious employee and, at the same time, nearly half of respondents admit the board not to have sufficient knowledge of information security. These outputs justify in part the insistence in literature to the importance of training employees and acknowledge all members of an organization including the Board (Boyce et al. 2011), (World Economic Forum, 2017) once *"Cybersecurity threats are universal, and board members have to take ownership of these risks. The topic should be discussed regularly in all board rooms, regardless of industry, region, or company size*" (Cheng and Groysberg, 2017). The level of board's information security knowledge might lead to a decreasing willingness to recognize the issue and to provide support, resulting on a

smaller portion for the cybersecurity budget. The latter is a crucial factor to stimulate and promote good practices culminating in the resilience of the firm.

This descriptive analysis allow the readers to understand how sectors within financial services industry are looking at the cybersecurity topic and how prepared they are to face a cyberattack. The undeniable reality is that cyberattacks are here to stay and each time they are more sophisticated. Moreover, there are new concerns related to the use of cryptocurrencies which enhances the importance of having a strong cyber protection.

Regarding the limitations of the sample, once the data was already collected, the author could not infer gender and age within the population. This study is not aiming for a generalization to a larger population but instead a study of how organizations see, react and prevent problems regarding cybersecurity. In fact, the main goal of this research was to bring a new perspective, a more directed view, from financial services industry and how its sectors are addressing cyber issues and preparing their organizations for this new reality. A significant point of this analysis is that a portion of respondents and one third of information security responsible belongs to the board of directors, meaning that they can influence decisions, promote awareness within the organization and establish good practices that may impact positively the firm. The author considers that an analysis with a younger target population within the organization and also out of it would be valuable to depict the perspectives and the evolution of the awareness within that population. Further limitations concern to the reduction occurred and expected in total cybersecurity's budget in the WAM sector. Further research could analyze if there are divergence factors that could lead to this result. Another suggestion of further research is to measure the impact of blockchains in cybersecurity.

Throughout the study, it seems to be a link between funding and cybersecurity effectiveness. For that reason, another avenue for further research would be studying

deeper the relationship between finance and organizations' funding and the level of cybersecurity practices implemented in these organizations. Perhaps, analyzing the relationship of government expenditures in this sensitive area and organizations' cybersecurity resilience would also be a relevant point.

The majority of cybersecurity-related decisions are based on a specific budget which is essential to ensure the protection of organizations and the increase of awareness practices. Budget constraints might have negative impact in the future of the organization. By allocating more funds in cybersecurity, more preventive actions might be taken. Consequently, the executive support could be improved leading to a more robust security.

Last but not least, the labor shortage in cybersecurity remains the big challenge for the next years. Skilled professionals demand is huge compared to its supply. Indeed, by 2021, it is predicted that there will be 3.5 million unfilled cybersecurity jobs and that cybersecurity unemployment rate will remain at zero percent (Cybersecurity Ventures, 2017). Therefore, the author would suggest a research measuring the impact of education and government incentives to this particular area in the dynamics of the labor market and perhaps a study to understand the role of human resources in cybersecurity.

7. References

Allen & Overy. 2017. “The EU General Data Protection Regulation,” 12. https://doi.org/10.1007/978-3-319-57959-7.

Amaral, Sandra. 2014. "O Papel dos Serviços de Informaçao no combate ao ciberterrorismo: O Caso Português".

Baldwin, David. 1997. The Concept of Security. Review of International Studies, 23(1): 5-26.

Boyce, Michael, Katherine Duma, Lawrence Hettinger, Thomas Malone, Darren Wilson and Janae Reynolds. 2011. “Human Performance in Cybersecurity: A Research Agenda.” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 55 (1):1115–19.

Catelli, Christopher, Barbara Gabriel, Jon Yates and Philip Booth. 2017. “Strengthening Digital Society against Cyber Shocks. www.pwc.gsiss.

Chang, Lennon YC and Peter Grabsky. 2017. "The governance of cyberspace". In "Regulatory Theory". Edited by Peter Drahos and published by ANU Press: 533.551.

Chang, Frederick., 2012. "Building a National Program for cybersecurity science. *The Next Wave:19,n°4:52.*

Cybersecurity Ventures, 2017. "2017 Cybercrime Report".

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. “Defining Cyber-Security.” *Technology Innovation Management Review*, 4(10):13–21.

Deibert, Ronald and Rafal Rohozinski.2010. Risking Security: Policies and Paradoxes of Cyberspace Security. DOI: 10.1111/j.1749-5687.2009.00088.x

Europol. 2017. *Internet Organised Crime Threat Assessment (IOCTA) 2017*. https://doi.org/10.2813/55735.

Fernandes, Filipe. 2013. "A Ciberseguraça e as Estruturas críticas: A GNR"

Franke Ulrik and Joel Brynielsson. 2014. “Cyber Situational Awareness - A Systematic Review of the Literature.” *Computers & Security* 46. Elsevier Ltd:18–31. https://doi.org/10.1016/j.cose.2014.06.008.

Hern, Alex. 2017. «NHS could have avoided WannaCry hack with “basic IT security”, says report». The Guardian. Acessed October 25. https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office

Hennin, Simon. 2008. “Control system cyber incident reporting protocol”. In: 2008 IEEE International Conference on Technologies for Homeland Security, HST'08. pp. 463-8.

Intelligence Community Assessment. 2017. “Assessing Russina Activities and Intentions in Recent US Elections: The analytic Process and Cyber Incident

Attribution". Accessed December 20. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Libicki, Martin, Liliab Ablon and Tim Webb. 2015. *" A Heuristic Cybersecurity Model". In " The Defender ' S Dilemma".Rand Corporation*

Libicki, Martin, David Senty and Julia Pollak. 2014. An Examination of the Cybersecurity Labor Market. In "Hackers Wanted". Rand Corporation.

Lipton, Eric. 2016. "The Perfect Weapon: How Russian Cyberpower Ivaded the U.S.". The New York Times. Published on December 13th of 2016. Accessed on December 15th. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=rank&module=package&version=highlights&contentPlacement=1&pgtype=collection

Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity

OECD Digital Economy Outlook 2017, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264276284-en

Klump, Ray and Matthew Kwiatkowski. 2010. "Critical Infrastructure Protection IV". Springer; 2010. pp. 113-26.

Miller, Nick. 2017. "The 11%; where are the women in cyber-security?". SC Media. Accessed November 22. https://www.scmagazineuk.com/the-11-where-are-the-women-in-cyber-security/article/579303/

Perez, Remi. 2010. "A Guerra no Ciberespaço: Princípios da Guerra Clássica Aplicados na Ciberguerra".

Petit, Harry. 2017 " What is WannaCry and who is behind it? Here's all you need to know about the ransomware that crippled the NHS". Mail Online. Published on May 12th, 2017. Accessed November 22th. http://www.dailymail.co.uk/sciencetech/article-4500614/All-need-know-ransomware-WannaCry-virus.html

Pierce, Adam. 2016. "Exploring the Cybersecurity Hiring Gap."

Ponemon Institute and Accenture. 2017. "2017 Cost of Cyber Crime Study," 56.

Porche, Issac, Jerry Sollinger and Shawn McKay. 2011. "A Cyberworm That Knows No Boundaries". In "A Cyberworm That Knows No Boundaries". Rand Corporation. 1–19.

Public Safety Canada. 2010. Canada's Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt- strtgy/index-eng.aspx

Rid, Thomas. 2011. "Cyber War Will Not Take Place". Journal of Strategic Studies 2011, pp. 1–28.

Singer, P. W., & Friedman, A. 2013. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.

Stark, J., and Fontaine D., 2015. “Ten Cybersecurity Concerns for Every Board of Directors.” *Cybersecurity Docket*.

The European Parliament, and The European Council. 2016. “General Data Protection Regulation.” *Official Journal of the European Union* 2014 (October 1995):20–30. https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

Walls, A. 2014. "Agenda Overview ofr Information Security Technologies and Services" ID:G00259776.

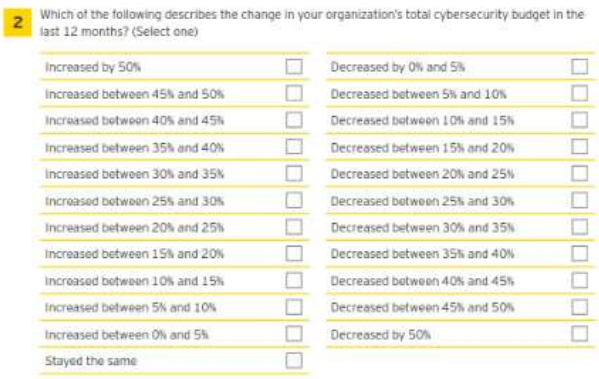
World Economic Forum. 2017. "The Global Risks Report" 12th edition.

Wiener, Norbert. 1948. Cybernetics: Or Control and Communication in the animal and the machine.

Zureich, Dan and William Graebe. 2015. "Cybersecurity: The continuing evolution of insurance and ethics". Defense Counsel Journal, April 2015: 192-198.

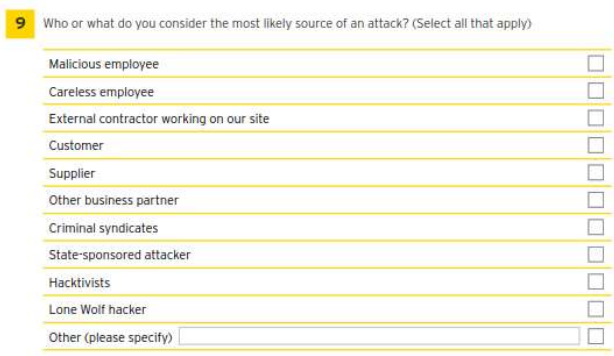
8. Appendix

Appendix 1 – Example of questions elaborated in the Global Information Security Survey 17-18.



2 Which of the following describes the change in your organization's total cybersecurity budget in the last 12 months? (Select one)

Increased by 50%	☐	Decreased by 0% and 5%	☐
Increased between 45% and 50%	☐	Decreased between 5% and 10%	☐
Increased between 40% and 45%	☐	Decreased between 10% and 15%	☐
Increased between 35% and 40%	☐	Decreased between 15% and 20%	☐
Increased between 30% and 35%	☐	Decreased between 20% and 25%	☐
Increased between 25% and 30%	☐	Decreased between 25% and 30%	☐
Increased between 20% and 25%	☐	Decreased between 30% and 35%	☐
Increased between 15% and 20%	☐	Decreased between 35% and 40%	☐
Increased between 10% and 15%	☐	Decreased between 40% and 45%	☐
Increased between 5% and 10%	☐	Decreased between 45% and 50%	☐
Increased between 0% and 5%	☐	Decreased by 50%	☐
Stayed the same	☐		

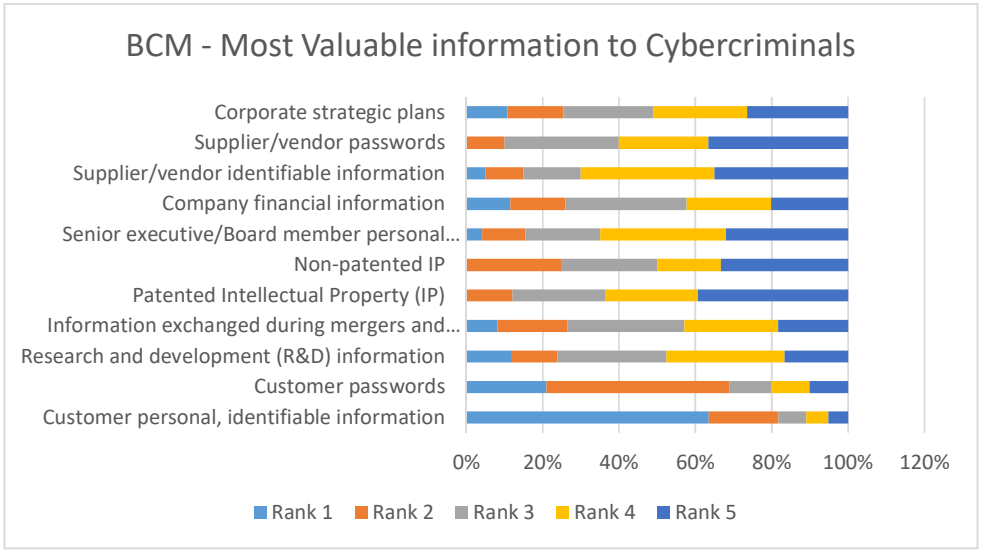


9 Who or what do you consider the most likely source of an attack? (Select all that apply)

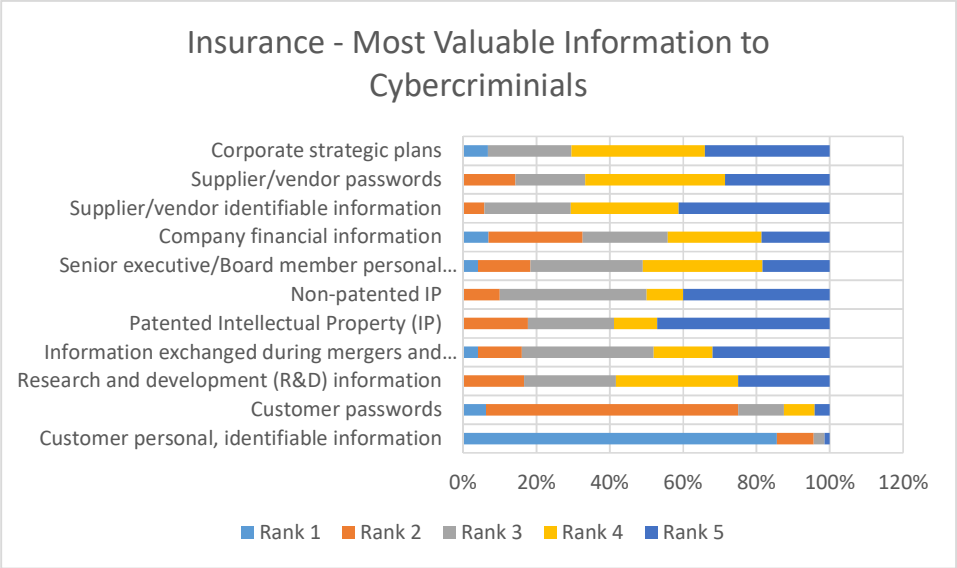
Malicious employee	☐
Careless employee	☐
External contractor working on our site	☐
Customer	☐
Supplier	☐
Other business partner	☐
Criminal syndicates	☐
State-sponsored attacker	☐
Hacktivists	☐
Lone Wolf hacker	☐
Other (please specify)	☐

Appendix 2 – Most Valuable Information to Cyber criminals:

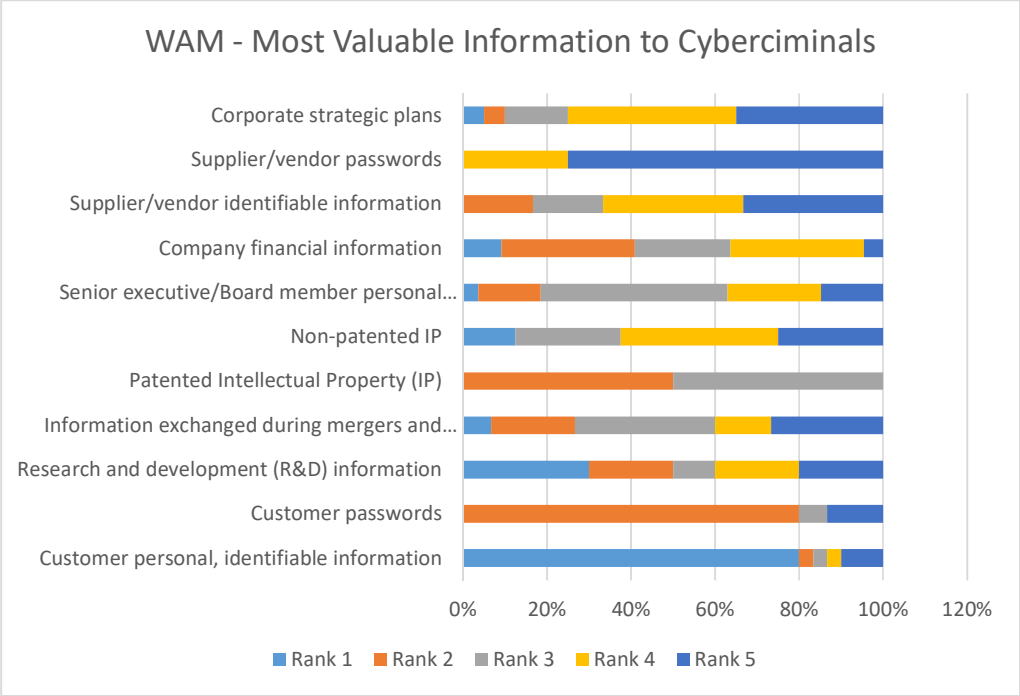
2.1. Banking & Capital Markets:



2.2. Insurance sector:



2.3. Wealth & Asset Management:



Appendix 3 – Likelihood of Detecting a Sophisticated Cyberattack