Cyber Security Solutions for Businesses in Financial Services:
Challenges, Opportunities, and the Way Forward

Shahzeb Akhtar, Symbiosis Centre For Management and HRD, Symbiosis International University (Deemed), India

Pratima Amol Sheorey, Symbiosis Centre For Management and HRD, Symbiosis International University (Deemed), India

Sonali Bhattacharya, Symbiosis Centre For Management and HRD, Symbiosis International University (Deemed), India

https://orcid.org/0000-0003-3069-1976

Ajith Kumar V. V., Skyline University College, UAE

ABSTRACT

This paper examines the challenges that small, medium, and large businesses in the financial services industry are facing concerning data security and providing relevant tools and strategies to protect the same. A qualitative research-based approach has been used where one-on-one interviews were conducted with 10 CIOs (chief information officers) and CISOs (chief information security officers). This data was compared with secondary data sources to validate the findings. This paper presents an in-depth analysis regarding security technologies and their efficacy to protect data assets and sensitive information. It will also opine about the technologies that each business type can use economically to cover the gamut of cyber-attacks. Existing research is restricted to either addressing small and medium businesses (SMBs) or large businesses. This paper attempts a comprehensive review for all sizes of businesses.

KEYWORDS

Cyber Threats, Data Security, Financial Services, Large Businesses, Security Technologies, Small and Medium Businesses

INTRODUCTION

Cyber threats are the reality for any business in this digital age. With technological advancement and people choosing an online data management, such as storing data on cloud-based platforms and sharing of important files and documents via servers, hackers get a chance to sneak into the systems, if appropriate security measures are not in place.

The purpose of this research paper is to understand the major cyber threats concerning small, medium and large organizations and the ways to mitigate them. This paper intends to answer questions such as: the most significant cyber threats impacting businesses, past cases of cyber threats, the financial industry scenario and the outlook towards such issues and steps to counter them.

Courtesy of Big Security in a Small Business World (Cisco.com)

The financial services industry has many players like the government, businesses and consumers. Financial services include banking, insurance, mutual fund, wealth management, stock markets, treasury/ debt instruments etc. The extent and nature of cyber threats vary depending on the size and type of services provided by the companies. In February 2016, a noted bank hack was executed, where $81 million were transferred from Bank of Bangladesh to accounts in the Philippines and Sri Lanka via Federal Reserve Bank through some payment messaging system (New York Times Magazine, 2018). In another cybersecurity breach in 2017, multiple computers were frozen worldwide by a ransomware attack, which exploited a vulnerability in a Microsoft portal to spread this self-propagating ransomware through public internet channels (NPR, 2017).

The average cost of data breaches, according to the Ponemon Institute, was around $3.86 million. According to Risk Based, about 4.1 billion worth records were breached in 2019 making 2019 the worst year so far. Every organization is creating a global network presence. Whenever such organizations adopt new technologies without sufficiently guarding against risks such as malware, data breaches, unsecured networks, they make their systems susceptible (Tawileh, Hilton and McIntosh, n.d.). According to BitGlass, 61.7% of records were leaked only in the financial sector in 2019. This was mainly because of Capital One mega-breach. A detailed breakdown of the types of breaches shows that around 75% of the breaches happened due to malware and hacking and around 18% of the breaches were due to accidental disclosures. Figure 1 depicts the top 5 cybersecurity threats that small, medium and large businesses (based on the number of employees) are currently facing. Large enterprises in India (https://msme.gov.in/know-about-msme) for example, are those enterprises which have more than INR 50 (USD 7 million) crore investment and annual turnover of more than 250 crore (USD 35 million); medium enterprises are those enterprises whose investment is more than INR 10 crore (USD 1.4 million) but less than INR 50 crore (USD 7 million)and annual Turnover is more than INR 50 crore (USD 7 million) but less than INR 250 crore (USD 35 million) and small enterprises are those enterprises whose investment is less than INR 10 crore (USD 1.4 million) and annual Turnover is less than INR 50 crore (USD 7 million).

If we closely analyze Figure 1, we see that ransomware is in the top category. Ransomware is a type of malware that encrypts the user's files. The attacker then demands a ransom payment from the user to restore access to its files and data. Research shows that such attacks can cause more than 24 hours of downtime (Scaife, Carter, Traynor and Butler, 2016). Moreover, stolen credentials are used to access critical data assets of an organization. Attackers commonly use phishing attacks (which

Figure 1. Top 5 Cyber threats for different size of businesses
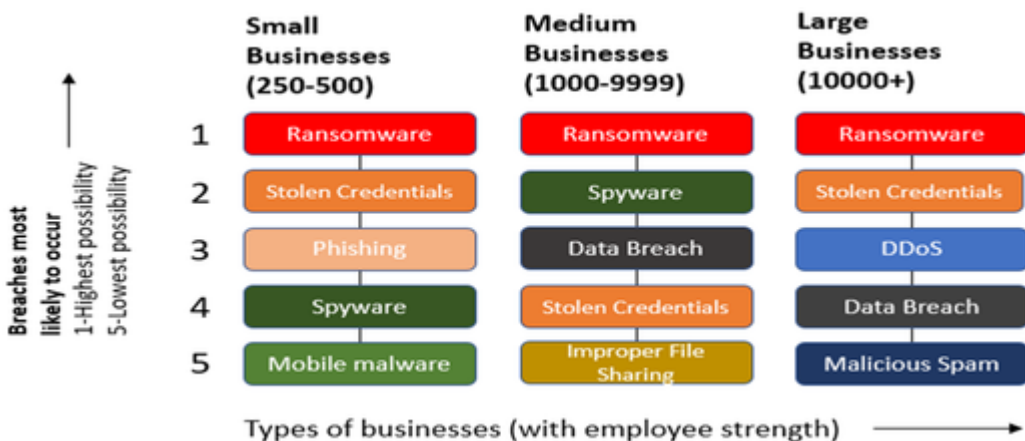
is about making emails and websites similar to the original one) for stealing credentials (Thomas et al., 2017). It is a cheap and effective tactic that involves deceiving employees. Data Breach is common in medium and large businesses whereas DDoS (Distributed denial-of-service) is unique to large businesses and not commonly seen with SMEs. DDoS is a situation when the attackers make a website or computer unavailable to the user by creating a flood of internet traffic causing a crash (Douligeris and Mitrokotsa, 2004).

LITERATURE REVIEW

The objective of the literature review is to understand different perspectives across journals and websites. The idea was to understand cyber threat vulnerabilities of small, medium, and large organizations.

According to Cyber Security Breaches Survey (2018), for large businesses, the average financial cost of data breaches was around £7260. The amount of attacks increase to two-third of large businesses. Most common attacks were fraudulent emails, along with impersonation and malware causing not just commercial but also reputational damage. This survey also shows that large firms face an average of 12 attacks per year, a medium-sized firm experiences an average of 6 attacks while a small firm faces a significant number of attacks. Moreover, the breaches were commonly found in organizations that held personal data and where employees used personal devices.

Qiu et al (2018) discuss about how mobile data sharing is very risky since it provides easy access to personal information. To solve this particular problem Qui et al (2018) came up with a model called Proactive Dynamic Secure Data Scheme (P2DS) that aims to protect data from unauthorized third parties. Wang et al (2019) propounded that financial loan management systems are generally not traceable and transparent, which allows cyber-attacks to take place. To overcome this, they suggested a loan on blockchain (LoC) which adds a layer of security while managing things digitally. Information Technology has developed a lot in the Financial Technology (FinTech) space as mentioned by Meng et al (2019). They talked about how passwords are the most widely used form of data protection and verification tool. But, that is also bypassed easily. So, they proposed a concept called Graphical Passwords (GP) as one of the promising solutions to replace the traditional password system. Nagurney & Shukla (2017) compare three different models for cybersecurity investment and different degrees of network vulnerability. In this particular research, qualitative properties are provided for the models with respect to financial services, varying degrees of cyber-attacks they faced and how they were countered. Donohue et al (2020) examines how the cashless society has transformed the traditional financial transactions. But, it is becoming quite tough to balance the risk of data privacy and security when a lot of data breaches are occurring. Therefore, concepts like block chain and card number randomization can help in mitigating the loss of data privacy. Elnagdy et al (2016) examine the importance of cybersecurity insurance in the financial sector due to the development of cloud-based solutions such as big data, which helps in mitigating the wide range of cyber security concerns and reduces the risk. Thakur et al (2015) point out that there is a fine line between cyber security and information security. They discuss that information security includes the aspect of people and ethics as well. Therefore, frameworks have been developed around these concepts to mitigate cyber risks. Li (2015) examines how the multi-firewall setup is quite sensitive and has network loopholes which can increase the cyber risk. This can be minimized by properly designing the network topology to prevent performance bottlenecks. Gai et al (2016) examine the problem that occurs with the classification of consumer related information that the financial services sector holds. Information which can be shared among various silos of financial institutions needs to be properly addressed. So, they came up with SEB-SIC model which works on the decision tree algorithm helping to classify various datasets. Packin (2018) addresses that Too-Big-to-Fail 2.0 is a valid concern since it does not matter how big a firm becomes, they need to have adequate security checks in place to sustain. Smeraldi & Malacaria (2014) discuss about the optimal spend on cyber security to make an appropriate budget.

But, the optimization algorithm and resources are non-linearly correlated. Romanosky (2016) shares the NIST framework for determining the cost of a cybercrime, which is essentially the cost of cleanup.

Baskerville, Spagnoletti, and Kim (2014) proposed that striking a balance between prevention and response strategies could prove worthwhile. Increasing network complexity requires a response-oriented security along with existing prevention strategies. Both paradigms should be given equal weightage. A comprehensive approach suggested by Bhasin (2007) describes that some basic security methods and defense tools can be used by the banking industry to mitigate risks caused by cyber thefts.

In a small business scenario therefore two strategies can be effective, one being risk assessment that includes identifying all possible threats and loopholes in the system and the other is regarding the review of security policies and procedures with constant vigilance. Paulsen (2016) examines that most small businesses don't even know what to protect. From the long list of cybersecurity recommendations, owners wrongly assume that if they select all the items, they will be well off. But that is not the case. It is critical to understand what to protect and what not to. The risk profile for a small business may be very different from a large one. Understanding the business functions before installing any security system is extremely crucial for the system to work with full efficiency.

Jenab & Moslehpour (2016) demonstrated a comparison regarding the password setups used by various sites and organizations. The study showed that more than 50% of them used the same password after the breach took place, whereas less than 40% tried a unique password setup. A password-cracking expert can use software that can try billions of possible combinations per second. This, unfortunately, makes passwords a large security threat. Ablon, & Libicki, (2015) discusses that security technologies are quite specific to each type of businesses with various organization sizes and so forth. The rise of digitization should motivate these firms to focus on protecting themselves.

Vavilis, Petković, & Zannone, (2016) examined that one of the major causes of a data breach is due to an inadequate measure for access to sensitive data. It is not always possible to bifurcate access control policies. Leakage incidents should be handled effectively, and understanding the severity of data breach incidents is quite important. So, the alert system should be prioritized efficiently. Rohn, E., Sabari, G., & Leshem, G. (2016) while examining the security practices for small enterprises, including enterprises with 10-50 employees also evaluated 67 different IT security tools. Small business owners were themselves not able to manage their security performance, which resulted in a higher number of data breaches. Bad management of data practice and lack of technical skills came out to be the top factors in higher data breaches.

Sangani & Vijayakumar (2012) discussed that large firms have their cyber security setup in place, whereas small and medium businesses (SMB's) do not take necessary steps to get the protocol set. SMB's generally don't have a dedicated IT team to implement and maintain the security tools present out there. In fact, most of the SMB's believe that data security is not even a concern for them. They are under the assumption that they are secure. New protection measures and protocols have been in vogue due to the rise of new threats in the market. Yet, SMB's don't pay attention to this problem. In most situations, SMB's are not fully aware of the security mechanism.

According to Netwrix 2017 IT Risks Report, two aspects had been covered. First is regarding cyber security risk comparison between large enterprises and SMB's and the second is about the top cyber security risks faced by the financial sector. If we delve deeper into the first aspect, we observe a comparative analysis in several aspects in large firms, only 33% do not have a dedicated IT team, whereas, in SMB's, around 73% do not have a separate IT team, this is a large number. Moreover, 65% of large firms focus on data security while 60% of SMB's prioritize endpoint protection. Furthermore, only around 25% of small, medium, and large businesses are well prepared for cyber thefts. The rest is unprotected. In terms of investment, around 72% of large firms and 42% of SMB's are willing to invest in cyber security solutions. The second aspect covers the risks of the financial sector. Around 64% of financial firms have a dedicated information security team. Also, 91% of financial firms have complete visibility into their user database. The main security focus is endpoints database and virtual infrastructure. As far as the main threat is concerned, 82% of the financial firm, consider

insiders with legitimate access, a major threat to information security. Financial organizations feel that major obstacles that they face are lack of budget, the complexity of IT infrastructure, and lack of time. Epps, C. (2017) discussed that as digitization proliferates, it brings so many opportunities for cyber thefts and hackers. With increasing cloud adoption and implementation of the Internet of Things, data are floating everywhere. It gives a lot of windows and openings to these hackers, which in turn can cause damage to the organizations.

Lagazio, Sherif, & Cushman (2014) proposed a system dynamic (SD) framework which works on the causal loop diagram (CLD) approach in terms of a data breach in the financial sector. The aim of the paper was to understand cyber theft impacts on the financial services industry at all levels. Findings revealed that changes in strategic priorities i.e. having consumer trust and loyalty, market position in comparison to its competitors are crucial factors in understanding the cost of cybercrime. The majority of the cybercrime cost is actually not driven by the number of incidents happening in the financial services sector, rather it depends more on what strategy do these companies choose, to protect their organization and how they position themselves amongst the other market players in a data breach situation (Anderson et al., 2013). Typically, companies do not strategize well and it results in overspending on cyber security technologies, and therefore they are unable to report appropriately to the internal and external stakeholders. Additionally, a financial firm's strategic response plays a vital role in ascertaining the cost of the data breach. Some factors which make the model weaker include poor policing, international frameworks are of weaker quality, jurisdictional arbitrage opportunities, increasing for cyber criminals all add to the increase in the cost of cybercrime. This in turn reduces the effectiveness of the model. The framework of this paper has strongly taken into consideration, the different levels of hierarchy between different tangible/intangible factors. Maisey (2014) discusses about the basic defence toolkit on which the enterprises rely. Things like antivirus, pattern-based detection, and prevention system, patching, and firewalls remain extremely important. But the cyber attackers are becoming more and more sophisticated in terms of new strategies used. So, this sophistication can infiltrate all kinds of defence toolkits which in turn is affecting every other organization across the globe. So, the security officers of various enterprises can learn from the past breaches and shift their focus from a reactive mindset to proactive management of perceived threats. This paper also talks about how a different approach towards these cyber thefts in terms of utilizing different types of tools and techniques helps to mitigate the threats. In the kill chain, the security officers of different enterprises need to focus on detection, denial, and degradation aspects. Intelligence analysis is something that needs to be kept in the core of all techniques used. Evaluation of current capabilities with the given reference architecture can help in solving the upcoming cyber security challenges. Kurpjuhn (2015) explained that SME's face threats similar to that of a large organization. When it comes to ground level investment in security technologies, the decision making becomes much tougher for the senior leader in terms of understanding the cost-benefit analysis. It has also compared the damage that is done to SME's and large firms. In terms of the gains achieved by hackers, the large firms are quite lucrative whereas the SME's are easy to penetrate. The top leeway that hackers are getting from SME's standpoint is the adoption of cloud-based services and usage of mobile networks. But, if proper protection parameters are not in place, it creates mishaps. So, Kurpjuhn (2015) proposed a unified solution concept – Unified Threat Management (UTM) solutions. These are a one-stop solution for SME's which consists of varied cyber security tools including cloud security, network security, VPN, content filtering, and many more providing 360-degree protection. More than installing this concept, understanding the management of it is quite important. Guiding the employees and planning out the charter in terms of streamlining the process for the organization can be useful.

Renaud (2016) took a survey of 110 Scottish SME's which shows that after any cyber-attack, companies face huge financial repercussions which may lead to shut down of businesses. Renaud also talked about how the government bodies helped SME's to understand threat messages and therefore what control mechanisms need to be followed. On analyzing the survey, it was found out that organizations generally take four kinds of security measures – Deterrent measures, Preventive

measures, Corrective measures, and Detection measures. The paper further explains how people respond when they receive a threat message. The most common reaction to such messages is to deny or reject them as they are not from trusted sources. Sometimes people do acknowledge such messages with the assumption that hackers cannot send them messages as they do not have digital assets. Therefore, a threat management model was derived based on existing models, which shows the entire cycle from the point an organization receives a threat message to the threat appraisal step where the organization needs to decide the coping strategy. Based on that, if they select neutralizing the threats, it directs them to the security system and precautions in place.

Choo (2011) discussed the threat landscape as a fast-moving environment and thus the level of preparedness was important. So, he proposed two ways in which organizations can manage cyber attackers. Firstly, he talked about the technical research aspect of government and third-party companies to significantly reduce the consequences and likelihood of cyber-attacks, by way of help in developing better security systems and improvising digital support. The success of such measures was dependent on the robustness of the system and the ease of use for easy implementation. He also talked about how these threats are evolving and becoming smarter with time. So, the solution needs to be innovative which can become a strategic driver in the value chain of the organization. Questions like how to address technical and operational issues associated with IT infrastructure during a cyber-attack, how to accurately identify and analyze a cyber-attack or a data breach in a stipulated time frame is important to be addressed. The second is an evidence-based policy approach where he discussed how important it is to conduct a strategic research and create evidence-based regulatory measures and compliances.

According to Property casualty (2018), the biggest breaches of history, such as Yahoo, Target and Equifax where around 145 million customer data, including social security numbers, their date of birth, addresses, contact details etc. Although these were large organization breaches, but this paper also states that small and medium businesses are more susceptible to security breaches. In this particular article, a set of guidelines have been explained for better prevention. One of the crucial aspects talked about here is the credentials and sensitive data held by employees of the firms. They use personal devices and unknowingly visit unauthorized websites which can compromise the credentials. In some cases where the employees have left the organization, the access to company's digital assets are not blocked. This should be taken into consideration. An employee who copies company's data into his personal drive is much more dangerous than cyber attackers themselves. Another thing is "sometimes free things cost the most". Employees make the mistake of using free Wi-Fi available at coffee shops and restaurants and they work with that Wi-Fi connection which can cause serious breaches of others using the same service. They also talked about how to keep alternate method in place once a data breach happens.

RESEARCH METHODOLOGY

For the research paper, the researcher has used a qualitative research method with the case study method to explore cyber security solutions in small, medium, and large businesses against major cyber threats. The sampling technique used here was 'Purposive Sampling' where a small group of people can logically represent a large population. The purpose was to capture the lived experiences experts who have dealt with cyber security related problems. The total respondents and their details are shared in figure 2 and Table 1. Researchers have illustrated that the qualitative research method is one of the valuable tools which creates meaningful insights (Bailey, 2014).

In this method, researchers try to understand the experiences and thought processes of the respondents. The themes generated by using this method helps in designing the framework for the paper (Yin, 2018). Defining the research question is extremely important. So, the central idea research question for the study is as follows: *What are the tools and strategies to reduce data breaches for small, medium, and large businesses?*

Figure 2. Research Framework
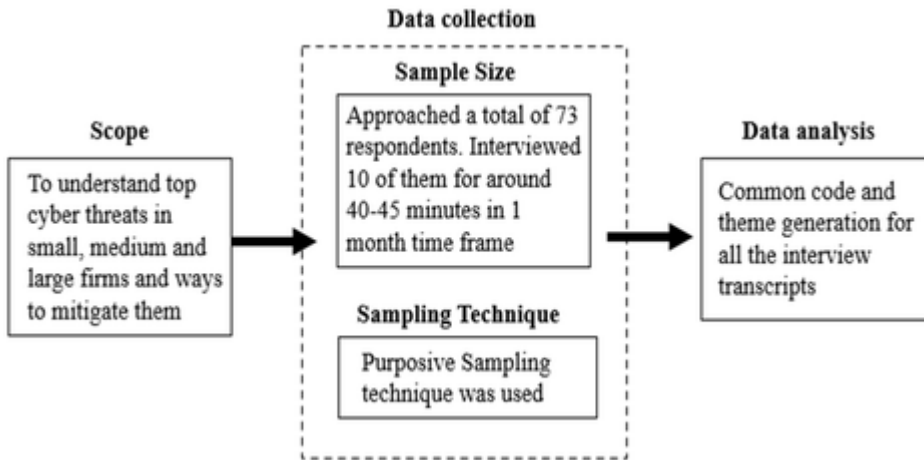
The above diagram (Figure 2) shows the flow of the research process undertaken.

In qualitative research, the researcher can reach data saturation with no new information available (Boddy, 2016). In this type of method, interviews are the major source for collecting data (Marshall & Rossman, 2016).

3.1 Data Collection

The data collection was a two-step process. The first step was sending out interview requests to Chief Information Security Officers, Chief Information Officers and Director of Information Security in various small, medium and large business units. The researcher tried connecting to 73 different respondents from various geographies and various financial firms through mails, messages through LinkedIn, and personal contacts. The second step was to schedule an online interview on a suitable platform such as Zoom/Google Meet/Cisco Webex where the interview was conducted. Out of the 73 approaches, 10 respondents agreed to an online meet. Detailed interviews were conducted with these respondents. Interview based approach was used just to explore:

- Top threats which impact different firms;
- The strategies they follow to protect their organization;
- Tweaking of strategy depending on the size of the firm;
- Role of cyber security providers in protecting the firms;
- Risk assessment and penetration tests to identify loopholes;
- Role of employees in the data breach.

They were asked around 9 open-ended questions during the interview, as part of the exploratory research. Interviews lasted for about 40-45 minutes in most cases. The major criteria for selecting a respondent were based on the position they hold, years of experience, working/worked in the financial services industry. Privacy was protected and no personal/private data were collected. Each respondent is abbreviated as alphanumeric codes (R1, R2,.....R12). They were quite generous and helpful in terms of taking out time for the interview and while responding to the questions posed to them.

3.2 Assumptions

The first assumption was that conducting interviews with 10 respondents and combining them with secondary data would be sufficient enough to reach data saturation. The second assumption was

Table 1. Demographic Profile

Respondent	Firm Size	Current Position	Years at current position
R1	Medium	CISO & DPO	1
R2	Medium	CISO	1
R3	Small	Senior Manager, Information Security	1
R4	Large	Cybersecurity Advisory Director	1
R5	Large	Director, Cybersecurity & Risk Services	1
R6	Large	CISO	5
R7	Medium	Project Manager & CISO	4
R8	Large	CISO	2
R9	Small	VP/CISO	1
R10	Small	CISO	2

that the interview participants shared honest feedback for the questions asked. Yin (2016) explained that participants tend to be truthful on calls and face to face interviews as because in this way the interview credibility increases.

3.3 Demographics

Table 1 shows the demographic break-up of the respondents.

3.4 Data Analysis

Analysis of qualitative data is divided into three steps - data reduction, display of data, and interpretation of data. All these steps are interrelated to each other and form an iterative process. Transcripts of the interview were put on a spreadsheet where different themes and patterns were identified (Miles and Huberman, 1994). Each transcript, which consisted of different words and phrases were scrutinized to create a list of non-overlapping statements (Moustaka, 1994). Researchers should correlate the findings of the research with the conceptual framework and gaps found in the literature review (Bogers et al., 2017).

RESULTS AND DISCUSSIONS

Based on the data that has been collected and analyzed throughout, the researcher has generated some themes which cuts across all the responses that we have received while interviewing the respondents. The 9 open-ended questions were converted into major research questions that guided us throughout the interview process.

These are the following research questions that guided the study:

Q1: Top threats, according to them, the strategies they adopted for their organization and how they train internal employees.
Q2: Strategy differences for each of the small, medium and large organizations.

Table 2. Themes for the research

Research Question	Themes
Q1	Phishing and ransomware is something which creates a lot of problems. Strategies may include internal setup or outside help.
Q2	Layered security approach should be followed for different sizes of Organization
Q3	They act as a strategic partner in terms of protecting the digital assets
Q4	Cyber security budget should be around 10-15% of the overall budget of the organization
Q5	Understand the risky areas while risk assessment and isolate the system when data breach happens

Q3: Role of cyber security companies and the importance of the tools these companies develop.
Q4: Yearly budget/cost for each size of firm.
Q5: The role of risk assessment and post attack measures.

There were themes generated for the questions as well, that is shown in Table 2.

Research Question 1: Top threats, according to them, the strategies they adopted for their organization and how they train internal employees?
Theme: Phishing and ransomware is something which creates a lot of problems. Strategies may include internal setup or outside help.

Seven out of ten respondents mentioned phishing and ransomware as the top cyber-attacks. All the respondents said that all these attacks are increasing every year as hackers are becoming more and more professional. Before carving out the strategy, the digital presence needs to be understood. Once we understand the online presence, we can plan as to what are the major areas needed to be covered.

R7 says: "Understanding the IT footprint plays an important role in terms of strategy planning, depending on how much data-intensive the work is".

Three respondents mentioned that the strategy differs from industry to industry. For a reseller, website becomes an important asset that needs to be protected. For a financial company, credit card information is something that needs to be safeguarded. On the other hand, for a manufacturing company, conserving supply chain data should be the top priority.

R5 says: "Sometimes, employees can be the biggest factor in terms of the data breach. Proper guidance and regular training can come a long way".

Two respondents mentioned that clicking on a wrong link can lead one to a fake website, similar to the original one. Once data is entered, it will show a glitch, and then it will redirect to the original page. By then, original data has been hacked by the cyber thefts. This is the concept of phishing attacks. So, training employees with basic cyber security guidelines regularly can be fruitful. This is done in terms of writing blogs, conducting contests, etc. One thing to keep in mind is to make

sure the technology is in place before blaming the employees. Once that is in place, employees can be looked after.

Research Question 2: Strategy differences for each of the small, medium and large organizations?
Theme: Layered security approach should be followed for different sizes of organization.

Eight out of ten respondents suggested that a layered based security approach is something that tends to make sense. Based on the revenue of the company, the IT budget, and the IT team, the company has, cyber security strategies for small, medium, and large organizations will vary. It is a three-layered approach that we are talking about.

First layer (Majorly for Small Businesses): Small organizations can implement this first layer of security. Having little/no toolset or skill set and with little budget and resources, companies need to be choosy in terms of getting value for money.

R4 says: "Knowing what we have in our IT infrastructure is very important. This will help in protecting the data for SME's much better".
Six respondents said that firstly, small businesses needs to have data encryption technologies in place. Additionally, an antivirus solution is something that needs to be set up because of limited resources. Moreover, endpoint security solutions such as setting up a complex password or multi-factor authentication can be a part of the first layer security solution.

Second Layer (Medium Businesses Can Opt This): Small or medium-sized firms can use this second layer of security technologies in addition to the first layer of security. Four respondents proposed things like baselining of servers, setting up a firewall around the network layer with lock management for firewalls, and approval mechanism for internal proxies.

R9 says: "EDR is one of the leading solutions for early threat detections. Although it is at a very nascent stage, bigger organizations are still trusting it at as an option"

Third Layer (Typically for Large Organizations): This is when organizations get bigger in size and digital data used. Here, the complexity of the cyber security environment increases.

R6 says: "Most large organizations try to build security systems internally. They have the money, they have the budget, which helps in tailoring to their needs".
Four respondents mentioned that the third layer of security solutions should include zero-trust security systems, advanced detection, and mitigation capabilities including log management and response timings.

Research Question 3: Role of cyber security companies and the importance of the tools these companies develop?
Theme: They act as a strategic partner in terms of protecting the digital assets.

Among the total responses, seven out of ten respondents said that cyber security companies such as CyberArk, FireEye, Fortinet which do a lot of R & D in terms of developing cyber security tools to prevent a data breach definitely adds a lot of value. Without them, no company can think of surviving. Hackers themselves come up with new tools to create new kinds of malware which can cause more damage. So yes, they play an important role.

R5 says: "Companies like CyberArk, Crowdstrike have very good solutions, but complex to manage and requires some knowledge to install it properly. This is where we (as CISO's) come to the picture".

R1 says: "There is never a 100% protection. Security is more about the experience than the tools itself".

Five respondents mentioned that the recommendations are given by cyber security companies, but it is managed by the IT team of the organization. So the ownership lies in the company's hand. It is like a strategic partnership between the two. Companies like CyberArk, who are completely in security tool making, has to be managed by the information security team of the firm. Things like zero trust, security systems are managed by the IT team. These cyber security solutions have to be analyzed and then implemented. So, the organization should first do the risk assessment and sizing the solution accordingly. Basic things like a backup of data at the cloud server should be done at the company end because the company cannot have a downtime of even a minute. There can transactions worth billions during that time.

Research Question 4: Yearly budget/cost for each size of firm?
Theme: Cyber security budget should be around 10-15% of the overall budget of the organization.

Budget is one of the trickier aspects that the organization needs to look at every fiscal year. Six out of ten respondents said that cyber security spending should lie within 10-15% of the overall budget. This will cover the implementation cost, the licensing cost, and the ongoing maintenance cost. Subscription cycles for these tools are generally from 1 to 3 years of the time.

R2 says: "I can have a million-dollar solution for my organization, but if I don't know how to implement it, it will just be a tool and do nothing. Hence, the value becomes zero".

Four respondents explained that small to medium enterprises (SME's) have higher cyber security spending as compared to large businesses. The reason is that large companies can survive regulatory impacts and compliance issues, which are regulated by the regulatory authorities and governance laws, but small and medium businesses cannot survive. The burden of the fine imposed tends to be very high to be paid out. It can even result in the collapse of the company. So, small businesses need to take extra care while working with customer data as well as third party data. Compliance requirement and the regulatory requirement are more in financial institutions as compared to other business industries. Also, we have to make sure that these tools are working cohesively with the network infrastructure.

Research Question 5: Role of risk assessment and post attacks measures?
Theme: Understand the risky areas while risk assessment and isolate the system when a data breach happens.

Six out the ten respondents discussed identifying risky areas in the IT infrastructure and isolating the systems attacked. Here, we are talking about two aspects- risk assessment and post-attack measures. Risk assessment covers three aspects-peoples, processes, and technology. First, we understand by analyzing the area which is riskier, based on that tool can be applied to fix the loopholes and windows from where cyber thefts can get entry points.

R7 says: "Gone are the days when you were doing monthly or quarterly risk assessment. Now, at a minimum weekly, best is when you deploy something latest or new. The vulnerability has to be tested on that day itself".

As far as post-attack measures are concerned isolating the system which has been attacked seems to be the best possible option immediately. Then we start identifying as to what percentage or of what magnitude the damage has been done and immediately start rectifying it. Communication is of the utmost importance here and it has to be done on a continuous basis. Intimating the stakeholders

(both internal and external) is important. Background work needs to be started quickly in terms of the restoration of data and try to set up new processes.

LIMITATIONS OF THE STUDY

Limitations were something that was present throughout the process. One of the biggest limitations which are faced was the telephonic interviews. A face to face interview is much more enriching in terms of personal connection, emotional build-up, understanding the body language and cues of the other person, which speaks a lot about them apart from the words they speak. That wasn't a possibility, so it is grateful that respondents gave the chance through an audio/video call. The researchers also found difficulty connecting to a larger sample as data was collected during Covid-19, when employees were teleworking and work responsibilities of cyber experts have increased manifold. Moreover, the time limit of the interview was a constrain for both interviewers and interviewees, as most of the interviews were through zoom meet. Length of interviews couldn't be extended beyond a limit. Each interview made the interviewers feel that additional interaction 5-10 minutes more would have been a valuable addition. Also, some people withdrew from the interview process due to some personal work, and the researcher couldn't get a chance to connect with them again. Note making and transcribing during interviews also were difficult. The majority of respondents did not prefer their interviews to be recorded, hence the researchers called off the idea of recording interviews. The company's spending on cyber security tools was something that respondents were reluctant to share. Apart from that, the process went smoothly. A

IMPLICATIONS

The findings in this study contribute majorly to academicians and corporate leaders in terms of takeaways that is offered. Bifurcating the findings into multiple themes gives a clear sense of understanding and clarity on various verticals of the topic.

First major contributions for academicians in this paper is a comprehensive overview across all sizes of firms, which can be used in various classroom programs for greater clarity to students. Secondly, this paper discusses about themes like layered approach and risk assessment, which can be widely used as a reference point for new research that happens in the future days to come. Our findings can best be depicted diagrammatically through Figure 3.

For corporate leaders, major contributions include the approach they can use to protect their IT infrastructure depending on their firm size. The findings also include the cyber security companies whom they can partner with and the budgets associated with it.

CONCLUSION AND FUTURE DIRECTION OF RESEARCH

A qualitative study is very helpful in understanding a person's experience throughout his work. The researcher analyzed using the qualitative exploratory study to understand strategies available for small, medium, and large businesses to reduce data breach. We interviewed 10 respondents who helped us in understanding how strategies differ, what role does cyber security companies play, and how does the investment differ.

In this paper, the researchers identified the top cybersecurity threats which were validated in the literature review as well as the findings that he analyzed for the interviews conducted. He was able to decode 5 different themes, each theme under a different research question which was developed as a part of the research methodology. Each theme addresses a unique aspect of the cyber security strategy, which can be used by researchers and organizations to their benefit. It was identified how phishing and ransomware (Scaife et al. 2016, NPR, 2017) are counted as a major threat in the financial sector

Figure 3. Proposed Cybersecurity Solution for Industry
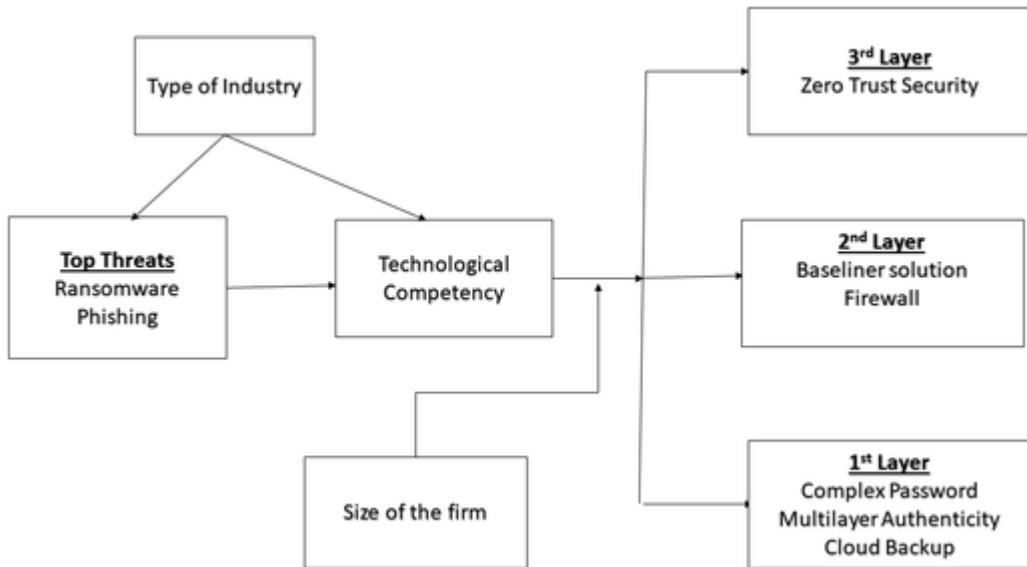
in particular and every other sector in general. It also uncovered how to layer security system-based approach can be a strategically smart move based on the investment capacity. An organization can anytime add a layer of security as they plan to scale up. Moreover, the researcher also understood how cyber security companies play a strategic role in terms of protecting the organization. But the firm needs to be active while monitoring the solutions provided by such companies. Additionally, we gathered the data that around 10-15% of the overall budget should be a bare minimum as far as cyber security setup is considered. Furthermore, we also discovered that risk assessment such as vulnerability assessment and post-attack measures need to be carefully monitored and analyzed so that a data breach can be stopped before happening itself. If it happens, the least possible damage occurs and the response time should be quick. Finally, employees play a major role in terms of the data breach that happens often. They need to be a bit more careful while clicking on links and responding to emails so that they don't end up giving a window to cyber thefts.

As far as the recommendations are concerned, researching about the number of data breaches happening and the major cases happened till yet can be helpful. Apart from that, research into any other business sector, such as eCommerce or Manufacturing can add a lot of value as part of the continuation to this research paper. Researchers can also opt for doing a quantitative research on this topic by understanding the effectiveness of the cyber security tools and quantify the efficiency.

Cyber-attacks will continue to perform illegal activities more and more in order to gain unauthorized access to computer systems and steal valuable information and data. By applying these tools in the right manner and with the right strategy will not only help in improving the financial data assets, but also help in raising the reputational credibility as well. Future researchers may wish to extend this study in other industries and carry out detailed surveys based research to test and validate the model suggested in figure 3.

ACKNOWLEDGMENT

REFERENCES

Ablon, L., & Libicki, M. (2015). Hacker's Bazaar: The Markets for Cybercrime Tools and Stolen Data. *Defense Counsel Journal*, *82*(2), 143–152. doi:10.12690/0161-8202-82.2.143

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Springer. doi:10.1007/978-3-642-39498-0_12

Bailey, L. F. (2014). The origin and success of qualitative research. *International Journal of Market Research*, *56*(2), 167–184. doi:10.2501/IJMR-2014-013

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151. doi:10.1016/j.im.2013.11.004

Bhasin, M. (2007). *Mitigating Cyber Threats To Banking Industry*. Available at: https://www.researchgate.net/profile/Madan_Bhasin/publication/286711208_Mitigating_Cyber_Threats_To_Banking_Industry/links/566d2c0608ae1a797e3e68e5/Mitigating-Cyber-Threats-To-Banking-Industry.pdf

Boddy, C. (2016). Sample size for qualitative research. *Qualitative Market Research*, *19*(4), 426–432. doi:10.1108/QMR-06-2016-0053

Bogers, M., Zobel, A. K., Afuah, A., Almirall, E., Brunswicker, S., Dahlander, L., & Hagedoorn, J. (2017). The open innovation research landscape: Established perspectives and emerging themes across different levels of analysis. *Industry and Innovation*, *24*(1), 8–40. doi:10.1080/13662716.2016.1240068

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. doi:10.1016/j.cose.2011.08.004

Cisco.com. (2020). *Big Security In A Small Business World 10 Myth Busters For SMB Cybersecurity*. Available at: https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-smb-cybersecurity-series-may-2020.pdf?CCID=cc000160&DTID=odicdc000509&OID=rptsc021237

Donohue, W., Afridi, Z., Sokolyuk, K., Bedwell, T., York, E. R., & Salman, A. A. (2020, April). Cashless Society: Managing Privacy and Security in the Technological Age. In *2020 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 1-6). IEEE. doi:10.1109/SIEDS49339.2020.9106653

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666. doi:10.1016/j.comnet.2003.10.003

Elnagdy, S. A., Qiu, M., & Gai, K. (2016, June). Understanding taxonomy of cyber risks for cybersecurity insurance of financial industry in cloud computing. In *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 295-300). IEEE. doi:10.1109/CSCloud.2016.46

Epps, C. (2017). Best practices to deal with top cybercrime activities. *Computer Fraud & Security*, *2017*(4), 13–15. doi:10.1016/S1361-3723(17)30032-5

Gai, K., Qiu, M., & Elnagdy, S. A. (2016, April). Security-aware information classifications using supervised learning for cloud-based cyber risk management in financial big data. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 197-202). IEEE. doi:10.1109/BigDataSecurity-HPSC-IDS.2016.66

GOV.UK. (2018). *New Figures Show Large Numbers Of Businesses And Charities Suffer At Least One Cyber Attack In The Past Year*. Available at: https://www.gov.uk/government/news/new-figures-show-large-numbers-of-businesses-and-charities-suffer-at-least-one-cyber-attack-in-the-past-year

Jenab, K., & Moslehpour, S. (2016). Cyber Security Management: A Review. *Business Management Dynamics*, *5*(11), 16–39.

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, *2015*(3), 5–7. doi:10.1016/S1361-3723(15)30017-8

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74. doi:10.1016/j.cose.2014.05.006

Li, J. (2015). The research and application of multi-firewall technology in enterprise network security. *International Journal of Security and Its Applications*, *9*(5), 153–162. doi:10.14257/ijsia.2015.9.5.16

Maisey, M. (2014). Moving to analysis-led cyber-security. *Network Security*, *2014*(5), 5–12. doi:10.1016/S1353-4858(14)70049-2

Meng, W., Zhu, L., Li, W., Han, J., & Li, Y. (2019). Enhancing the security of FinTech applications with map-based graphical password authentication. *Future Generation Computer Systems*, *101*, 1018–1027. doi:10.1016/j.future.2019.07.038

Miles, M. B., & Huberman, A. M. (1994). Qualitative Data Analysis: An Expanded Sourcebook. *Sage (Atlanta, Ga.)*.

Moustakas, C. (1994). *Phenomenological research methods*. Sage. doi:10.4135/9781412995658

Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588–600. doi:10.1016/j.ejor.2016.12.034

Netwrix. (2017). *IT Risks Report*. Available at: https://www.netwrix.com/2017itrisksreport.html?_ga=2.8870384.479892311.1593093370-2039205455.1593093370

Npr.org. (2017). *NPR Choice Page*. Available at: https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday

Nytimes.com. (2018). *The Billion-Dollar Bank Job*. Available at: https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html

Packin, N. G. (2018). Too-Big-To-Fail 2.0? Digital Service Providers. *Indiana Law Journal (Indianapolis, Ind.)*, *93*(4), 7.

Pages.bitglass.com. (2019). *The Financial Matrix Bitglass. Financial Breach Report*. Available at: https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_Financial_Matrix2019.pdf?aliId=eyJpIjoidEFtUm1uM09HdGtOVTIySiIsInQiOiJ2dWU4Y3NLMlFybWMyb1wva21wNVvpkQT09In0%253D

Paulsen, C. (2016). Cybersecuring Small Businesses. *Computer*, *49*(8), 92–97. doi:10.1109/MC.2016.223

Propertycasualty360. (2018). *Playing It Safe: Cybersecurity For Small- To Medium-Sized Businesses*. Available at: https://www.propertycasualty360.com/2018/01/25/playing-it-safe-cybersecurity-for-small-to-medium-sized-businesses/?slreturn=20200530012145

Qiu, M., Gai, K., Thuraisingham, B., Tao, L., & Zhao, H. (2018). Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Generation Computer Systems*, *80*, 421–429. doi:10.1016/j.future.2016.01.006

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud & Security*, *2016*(8), 10–18. doi:10.1016/S1361-3723(16)30062-8

Rohn, E., Sabari, G., & Leshem, G. (2016). *Explaining small business InfoSec posture using social theories*. Information & Computer Security. doi:10.1108/ICS-09-2015-0041

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. doi:10.1093/cybsec/tyw001

Rossman, G. B., & Rallis, S. F. (2016). *An introduction to qualitative research: Learning in the field*. Sage Publications.

Sangani, N. K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informações Econômicas*, *16*(2), 58.

Scaife, N., Carter, H., Traynor, P., & Butler, K. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. doi:10.1109/ICDCS.2016.46

Smeraldi, F., & Malacaria, P. (2014, May). How to spend it: optimal investment for cyber security. In *Proceedings of the 1st International Workshop on Agents and CyberSecurity* (pp. 1-4). doi:10.1145/2602945.2602952

Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. *ISSE/SECURE 2007 Securing Electronic Business Processes*, 331-339. <ALIGNMENT.qj></ALIGNMENT>10.1007/978-3-8348-9418-2_35

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cybersecurity threats and security models. In *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing* (pp. 307-311). IEEE. doi:10.1109/CSCloud.2015.71

Thomas, K., & Li, F. (2017). Data Breaches, Phishing, or Malware? *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. doi:10.1145/3133956.3134067

Vavilis, S., Petković, M., & Zannone, N. (2016). A severity-based quantification of data leakages in database systems. *Journal of Computer Security*, *24*(3), 321–345. doi:10.3233/JCS-160543

Wang, H., Guo, C., & Cheng, S. (2019). LoC—A new financial loan management system based on smart contracts. *Future Generation Computer Systems*, *100*, 648–655. doi:10.1016/j.future.2019.05.040

Yin, R. K. (2016). *Qualitative Research from Start to Finish*. The Guilford Press., doi:10.1111/fcsr.12144

Yin, R. K. (2018). *Case study, research and applications: Design and methods* (6th ed.). Sage Publications.

Shahzeb Akhtar is pursuing MBA from SCMHRD in the field of Sales and Marketing. He has been a winner and finalist of various corporate competitions. He has done his internship from Capgemini.

Pratima Sheorey did her MBA in Marketing from the University of Pune and has more than 17 years of experience in the academic and corporate sector. She has worked with ORG-MARG (now ACNielsen), the Hero Group and others in the corporate sector and has been a faculty at various Institutes of Symbiosis International University (SIU).She has worked in the area of Market Research, Training & Consulting and Business Development. Pratima has trained executives in many organisations in India and abroad in various behavioral and functional programmes like Service Orientation, Selling Skills, Creativity and Innovation etc. across levels. She has published many papers in reputed journals and participated in many conferences in India and abroad. Research interests: Customer Engagement, Experiential Marketing, Consumer Behavior, Value Creation, Co-creation of value by customer, etc.

Ajith Kumar V. V. has done his Ph.D. in the area of Industrial Relations and has done his MBA in Human Resource Management from Andhra University. He has undergone a course on Cross Cultural Management & Problem Solving from Nanyang Technological University, Singapore. His research areas are Leadership, HR flexibility, Business Ethics and Diversity Management. He has conducted many executive programs in the areas of Leadership, Conflict & Negotiation to employees of corporates like Gulf air, Wipro etc. He has more than 20 years of teaching experience in reputed business schools like ICFAI, Symbiosis Institute of Business Management in India. He also worked as a faculty member at Bahrain Training Institute in the Kingdom of Bahrain for one year. He teaches business subjects like Human Resource Management, Organizational behavior, Strategic Management, Business Ethics Leadership, and Innovation. He believes in core values of teamwork and trust.