Cyber Risk for Small and Medium-Sized Enterprises

The Janet & Mark L. Goldenson Center for Actuarial Research

University of Connecticut

August 2016

Table of Contents

Introduction

Cyber risk is any risk or financial loss, disruption or damage to the reputation of an organization from any type of failure within their information technology systems. Cyber risk is not a new concept in modern society but many companies, especially small and medium-sized enterprises may not be aware of the real and devastating consequences of a cyber-attack. Imagine all or even some of your company's confidential information becoming public knowledge. How would your employees, customers, and clients feel? It would compromise the integrity of your entire business; ruining current and future opportunities. As companies of all sizes increase their dependency on information technology, potential technology breaches increase. Most large businesses have already incorporated cyber risk management into their business strategy because there is a broader awareness of the need for holistic and thoughtful protection from cyber threats. However, unlike large businesses, small and medium-sized enterprises (SMEs) generally do not regard cyber risk as a strategic component in their business model despite the fact that cyber risk for SMEs is a real and growing phenomenon. An SME is generally defined by the U.S. Small Business Administration as one that is "privately owned and operated, with a small number of employees and relatively low volume of sales". While the legal definition of what constitutes a small business varies according to industry, for most businesses to qualify for federal SBA programs, they must have fewer than 500 employees. Based on this definition, SMEs represent the largest sector of the US economy that is exposed to cyber risk. However, it is the smaller end of the SME spectrum, which is the focus of this article. These are SMEs where risk management in general is not an integral component of the business, and there exist no formal policies or procedures on cyber risk management.

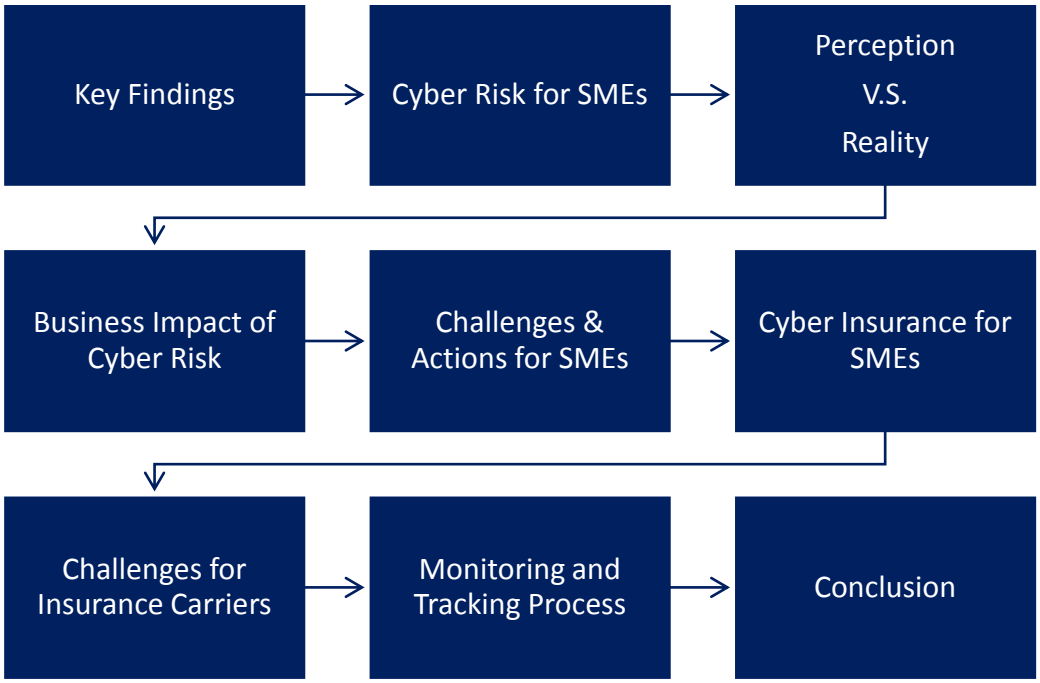
As an example, we will illustrate the fate of "Rokenbok Education", a small public benefit company dedicated to developing applied technology and engineering learning experiences for K-12 students. In 2015, Rokenbok Education suffered a malware infection to their data during their busiest time. Hackers had encrypted their company files, making them unusable, and demanded a hefty ransom to restore the

data. Because Rokenbok Education didn't have a cyber risk management strategy, they had to restructure their business to avoid paying the ransom. Although they eventually overcame the cyber threat, in two days Rokenbok Education lost thousands in sales and a lot of customer loyalty. Rokenbok Education isn't alone. According to Timothy C. Francis, enterprise leader of cyber insurance at Travelers, sixty percent of all online attacks in 2014 targeted small and midsize businesses. (New York Times)

In our report, we utilize a rigorous review of existing literature to analyze cyber risk as it pertains to SMEs, and analyze various mitigating strategies to protect against cyber risk.

Executive Summary

In an era of rapidly expanding knowledge and technology, businesses are forced to rely more and more on technology to accomplish everyday jobs. Although these day to day technology advances help businesses function at a higher level of productivity, it also exposes them to many risks. Unfortunately, SMEs are the target of many cyber-attacks because they are not aware of the severity of these attacks and do not have the proper security measures in place. This report follows a step by step process on how SMEs can incorporate a cyber risk management plan, including purchasing cyber insurance, into their business to protect themselves from cyber-attacks. The report that follows can be summarized in the flowchart below.



In our study, our key findings are as follows:

- Cyber risk is a real and growing concern for SMEs.

As SMEs integrate new technology into their business, their cyber risk exposure increases. Businesses must develop an understanding of what cyber risk is and the extent of their recent exposure as it pertains to their business sector.

- SME perceptions of cyber risk may not be an accurate measure of what the actual reality for cyber risk is.

More than half of the SMEs haven't realized that they have inadequate protection from cyber threats (KPMG). While some SMEs are aware of these threats, they do not think that additional preventive measures must be taken to protect themselves as reflected in the budget allocated to IT spending (SANS).

- The impact of cyber risk for SMEs is significant.

Once a business has developed an understanding of what cyber risks are, it is important that they are able to assess the potential impact that a cyber breach can have on the company. The impact for SMEs may be

different than the impact for large businesses, and likewise, an impact for one SME might not be a concern for another SME. However, in either case, the cyber risk impact for SMEs is very significant as described in the detailed report below.

- SMEs are facing many challenges in the process of reducing their cyber risk.

Because cyber risk is difficult to understand, most SMEs lack knowledge of cyber risk and have an inadequate ability to handle these cyber risk threats on their own. Also, there are myriad cybersecurity solutions available in the market, but SMEs do not have access to reliable guidance on how to create a robust cyber risk management plan. The last challenge is that although cyber insurance is considered a cybersecurity solution, cyber insurance is not easily accessible to SMEs.

- SMEs can take certain steps to reduce cyber risk

There are certain individual actions SMEs can take like improving IT security, operational efficiencies, etc. to reduce their cyber risk exposure after assessing what the potential impact a cyber breach can have on a business. SMEs must also decide if it is in their best interest to purchase some type of cyber insurance coverage to ensure more comprehensive cyber risk protection.

- Overall, cyber insurance is a growing market, but cyber insurance for SMEs is only slowly expanding.

Less than 3 percent of SMEs have cyber insurance whereas 40 percent of large businesses have cyber coverages. (Aon)

- There are many challenges involved with offering cyber insurance for SMEs.

Cyber insurance coverage will have to differ based on SMEs needs, by business sector and the operational security level maintained by the SME. It should also be comprehensive and affordable.

- ➢ To grow and develop the cyber risk insurance market for SMEs and to ensure it is profitable and viable, it is important for insurers to track and monitor both the frequency and severity of cyber risk for SMEs.

The remainder of the report breaks down each step, detailing methods, statistics, and potential problems that can occur during each phase. The main focus is SMEs, but often references are made to large businesses to expose parallels, and to make estimates of cyber risk costs and cyber insurance needs for SMEs.

Defining Cyber Risk

Many studies refer to cyber risk as "operational risks to information and technology assets that have consequences affecting the confidence, availability, or integrity of information or information systems" (Cebula and Young) (Copula) (Biener). Among these studies, cyber risk is categorized as an operational risk that a company may undertake during their business operations. This raises the question, what is an operational risk? Operational risk is defined as losses to a company due to internal process failure or external events during business operations. (Lopez)

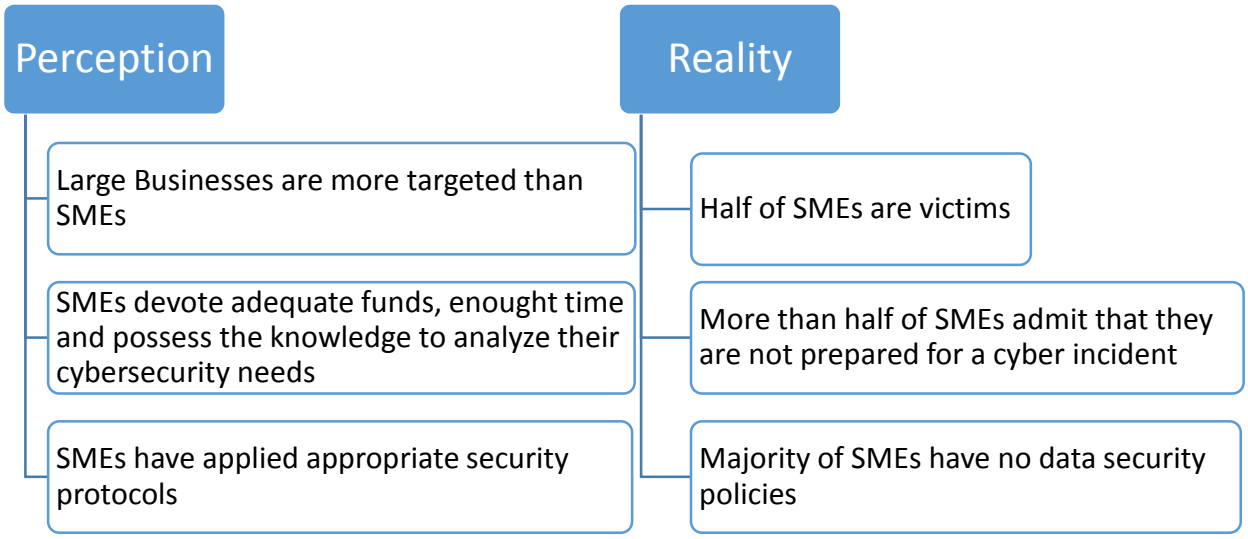
James Cebula and Lisa Young recently broke down and classified cyber risk into four classes based on businesses of all sizes. The four classes are Attack on Physical Systems, Authentication and Privilege Attacks, Denial of Service, and Malicious Internet Content. (Cebula and Young) However, the focus of our report is on cyber risk for SMEs, so in this section, we will define and analyze the types of cyber risk that most SMEs face, as well as break down cyber risk for SMEs as follows:

Attacks on Physical Systems	Attacks on physical systems include hardware attacks from laptops, computers, tablets and hard disks. Other attacks include unprotected endpoints

	attacks from USB devices and other removable media, server room break-in, internal network hacking and monitoring by unauthorized third parties. (GFI)
Authentication and Privilege Attacks	Authentication and privilege attacks include insufficient password requirements, disgruntled employees, high privileged accounts, and privilege creep. It usually happens due to inappropriate cybersecurity protocols. (GFI)
Denial of Service	Denial of service includes natural disasters such as connection downtime and power cuts. Targeted denial of service such as bandwidth exhaustion, vulnerable service attack, and single point failures is usually caused by over-depending on a person or a couple of individuals. Other types of denial of service include inadequate prevention from cyber incidents and lack of proper documentation. (GFI)
Malicious Internet Content	Malicious Internet content includes social engineering such as phishing attacks, malware caused by viruses, Trojans, and worms,

	inappropriate drive-by downloads to company technology, and web application attacks. (GFI)

Perception vs Reality



With a proper definition of cyber risk, it is easier to view the misconceptions between what SME owners believe and the reality of the cyber threats that SMEs are faced with. Most SMEs feel that it is unlikely that they will be targeted due to their size and cybercriminals would opt to target a larger business instead. As seen in figure 1, 85 percent of SMEs believe that large businesses have been targeted more often than SMEs have. (NCSA) In the PWC survey, SMEs believe that the frequency of cyber incidents will decrease in later years. (PWC)

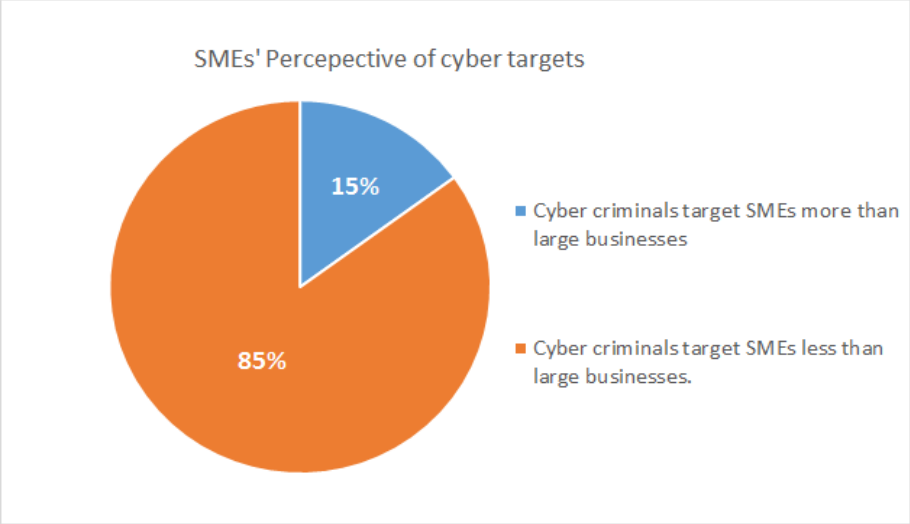


Figure 1. Reproduced Courtesy of (NCSA)

However, in reality, SMEs are a potential and growing target for cybercriminals. In 2014, 50 percent of small businesses reported that they have been a victim of a cyber-attack. (NSBA) Due to the increase in the occurrence of cyber-attacks, cybersecurity is becoming a growing concern for small business owners. As seen in figure 2, the allocation of phishing attacks on SMEs has grown significantly from 2012 to 2014. (Prevalent) This reinforces the fact that cyber criminals do not discriminate between large businesses and SMEs, as long as it is profitable and lucrative. They will target any entity that has valuable data and a weak security system. Examples include credit card information and social security numbers. Therefore, information that SMEs are currently holding has significant value to cyber criminals.

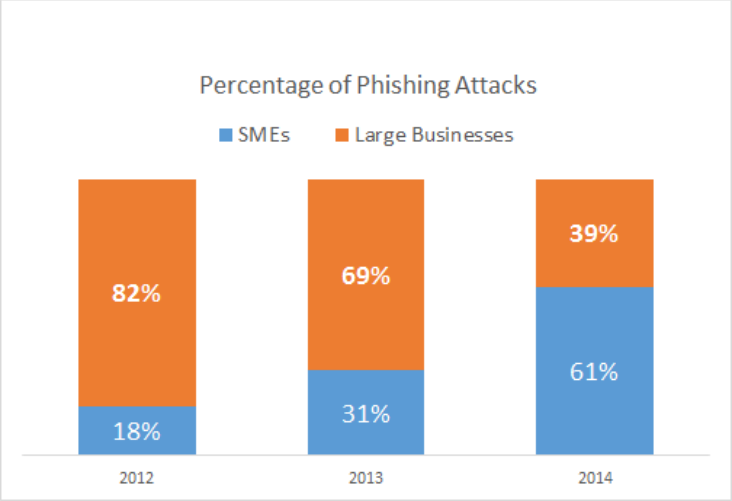


Figure 2. Reproduced Courtesy of (Prevalent)

Another perception is that SMEs are devoting a sufficient amount of time and money into cybersecurity. In the NCSA (National Center for Supercomputing Applications) survey from 2012, most SMEs believed that they have already applied appropriate security protocols to protect their business from potential cyber-attacks. As seen in figure 3, most SMEs considered that they do have adequate funds to invest in cybersecurity, they do have enough time to devote to cybersecurity, and they do possess the skills and the knowledge to analyze their cybersecurity needs. (NCSA).

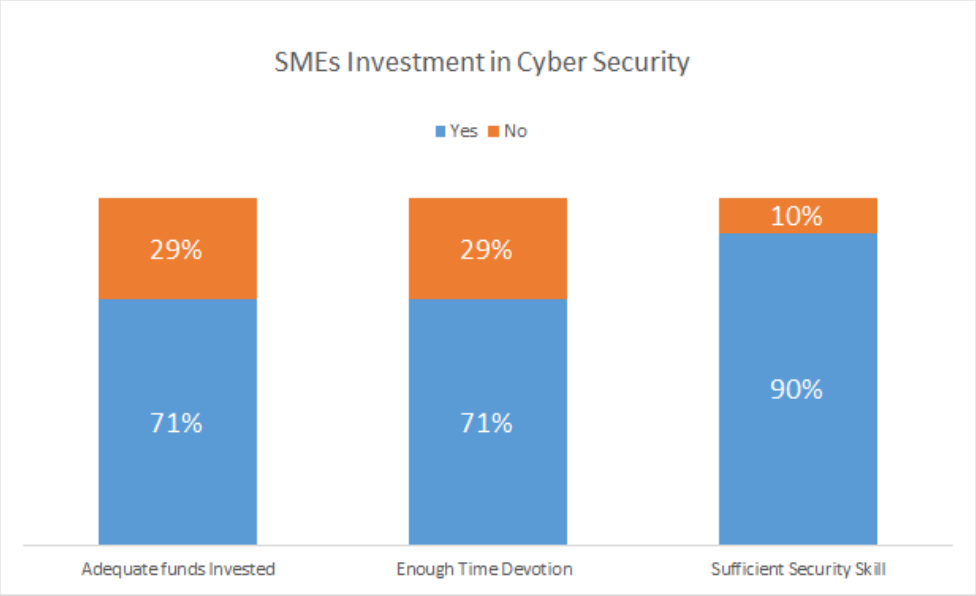


Figure 3. Reproduced Courtesy of (NCSA)

However, the reality is different. More than half of SMEs admit that they are currently not prepared for a cyber incident and are concerned that a cyber incident will have an impact on their business. (KPMG) SMEs generally have inadequate resources and devote less time and money to cybersecurity when compared to large businesses. (NCSA) As shown in Figure 4, the IT budget for large businesses will increase in 2016 whereas the IT budget for SMEs will remain constant. (SANS) In addition, both United Nations Office on Drugs and Crimes and NCSA surveys said that about 67 percent of SMEs have no data security policies at all, and out of the 33 percent with data security policies, 87 percent of them do not have their policies formally written. (United Nations Office on Drugs and Crimes) (NCSA) If a cyber incident takes place, SMEs will be vulnerable due to their poor investment in cybersecurity and their lack of appropriate cyber policies.

IT Security Spending Trends		
	2015	2016 (Projected)
Large Businesses	$1M-$10M	$10M-$50M
SMEs	$100K-$500K	$100K-$500K

Figure 4. Reproduced Courtesy of (SANS)

Business Impact of Cyber Risk

Out of the SMEs that have had a cyber breach, ninety-three percent experienced a severe impact to their business. (KPMG) In general, cyber impact cost for SMEs increased 239 percent from $8,699.49 to $20,751.97 on average in 2014 (NSBA). Furthermore, 60 percent of SMEs will close within six months after a cyber-attack. A more detailed analysis of other potential consequences such as reputation damage, loss of clients, customer delay, business' ability to operate, time to recover, loss of money and savings, and business failure follows:

- Reputation Damage

SMEs need a strong reputation to become long lasting companies. (Temi & Christine) As seen in the KPMG survey, SMEs do not think cyber incidents will affect their reputation. (KPMG). However, cyber incidents do have an impact on their reputation. SMEs who suffered from cyber breaches have damaged their reputation by 31 percent. (KPMG) In this survey, KPMG defined reputation damage as the loss of clients, the ability to attract new employees and the ability to win new business.

- Loss of Clients

For all businesses, clients are the fundamental key to success. Losing clients suggest that their business is less competitive compared to other businesses. In a survey conducted by RAND, after a cyber breach, one in ten customers will stop conducting business with the company, and one in four customers will give them less business. (RAND) Likewise in the KPMG survey, 4 in 5 consumers are concerned about which businesses have access to their data and whether the data is safe. (KPMG). Hence any cyber breach could significantly reduce customer confidence in the business and a potential increase in loss of clients.

- ➢ Customer Delay, Business Ability to Operate and Time to Recover

According to the KPMG survey, 26 percent of SMEs have experienced a customer delay due to a cyber breach. Delays such as businesses websites being offline are the most typical. Other delays such as an inability to operate due to the lack of access to the business database can often lead to frustration for both the customer and the business. (KPMG) According to the 2015 NSBA survey, after a cyber breach, 48 percent of SMEs incurred a service interruption that damaged their ability to operate. (NSBA). Other consequences such as paying someone else to fix the issue, and possible legal fees inhibit the business from running smoothly. (KPMG)

Recovery time has a direct correlation with customer delay and business interruption. The longer it takes to get back to normal, then the longer it takes for customers to conduct business with the company, which in turn creates a longer business interruption. This cycle will also indirectly impact the company's reputation and customer loyalty. As seen by the data in figure 5, there is an increasing trend in the time required to resolve cyber-attacks. (NSBA)

	AUG. 2013	DEC. 2014	DEC. 2015
Less than 1 day	38%	30%	25%
Between 1 - 3 days	39%	34%	34%
Between 3 - 7 days	11%	14%	15%
More than a week	7%	9%	10%
More than two weeks	5%	13%	16%

Figure 5. Reproduced Courtesy of (NSBA, 2015)

In general, any form of customer delay or business interruption could have a negative impact on a business.

- ➢ Loss of Money and Savings

The most common target for cyber-attacks is sources of liquidity. SMEs are facing a huge increase in the amount of money stolen from their bank account caused by cyber-attacks in recent years. According to the 2014 and 2015 NSBA surveys, the average amount stolen from an SME bank account increased from about $6,900 in 2013 to about $32,000 in 2015, representing a 462 percent increase. (NSBA) Furthermore, even if the SMEs can file for fraud and get their loss refunded, the damage on their business has already been done.

- ➢ Business Failure

There is no one cause that is directly related to business failure, rather a combination of the causes listed above. A combination of brand damage, loss of clients, customer delays, ability to operate, time to recover, and loss of money fuels the fact that 60 percent of SMEs will close within six months after a cyber-attack. (NCSA)

Challenges and Actions to Reduce Cyber Risk for SMEs

Not only is the business impact huge, but there are many challenges to overcome. The cyber risk that SMEs are currently facing is a very complicated risk. In our previous analysis, we identified four general cyber risks: “Attacks on Physical Systems”, “Authentication and Privilege Attacks”, “Denial of Service” and “Malicious Internet Content”. (GFI) Each of these four categories is complex in its own unique way. Due to the complexity that is entailed in each category, it is a straining task for an SME to master the concepts, and effectively use that knowledge to protect the business from a cyber breach.

Another level of complexity is that SMEs have many different types of business sectors, such as financial services, retail stores, medical healthcare, administrations, technology and software, education, and other smaller groups. (NetDiligence) Figure 6 below shows the market size of each business sector. Different SMEs business sectors are exposed to different types of cyber risk and different frequencies of cyber breaches. As seen in figure 7 below, frequency of cyber breaches varies by business sector. For example, medical healthcare companies, which make up 11 percent of the SME business sector, represent 44 percent of all breaches. The stolen data is usually pertaining to social security numbers. Loss of these critical numbers can often lead to identity thefts. Thus, another challenge SMEs face is to establish a cyber risk management plan catered to characteristics of their unique business sectors.

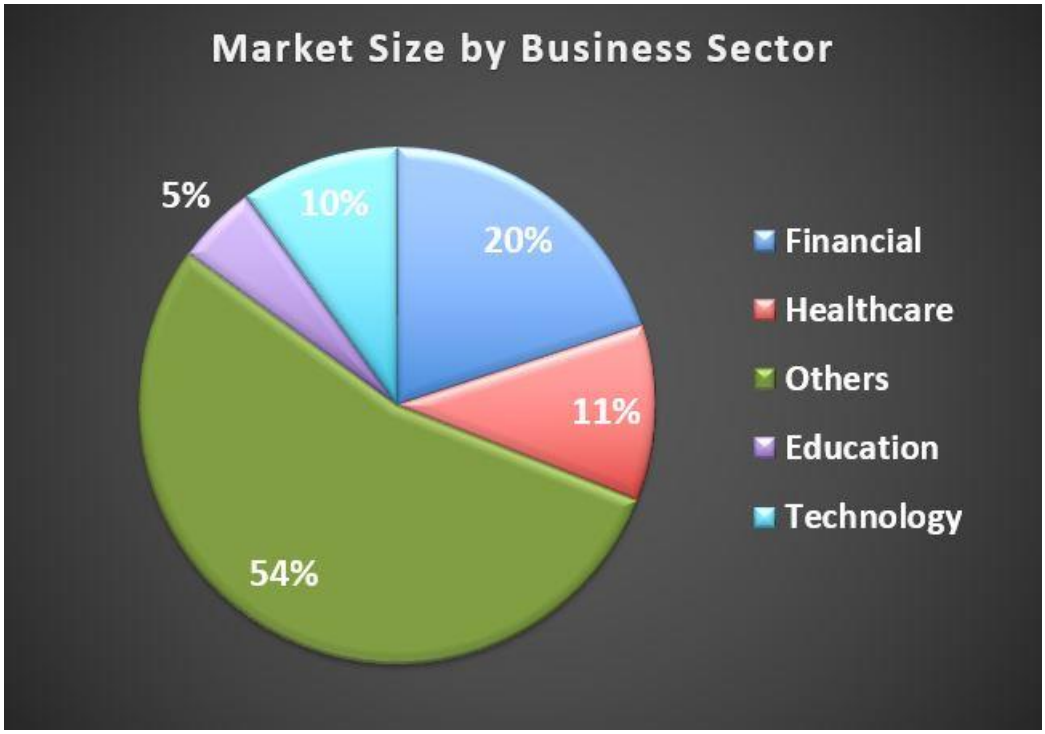


Figure 6. Reproduced Courtesy of (Ponemon)

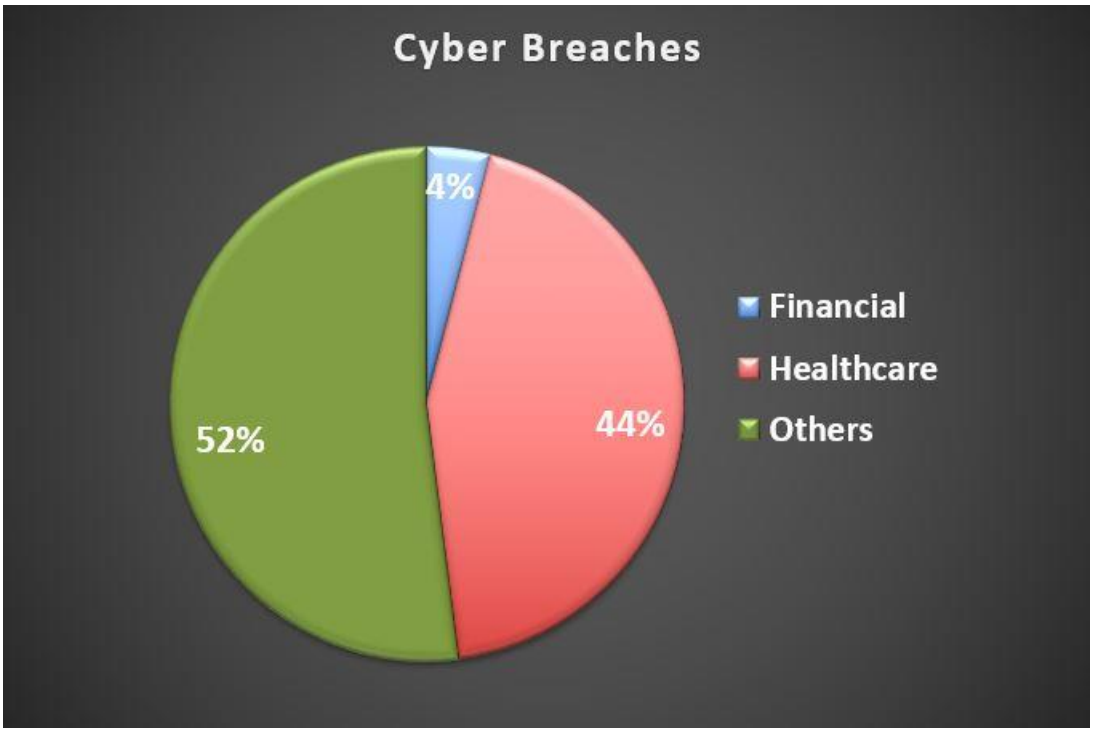


Figure 7. Reproduced Courtesy of (III)

Additionally, there are countless cybersecurity options available in the market. You can avoid certain types of cyber risk by installing antivirus software, identifying potential cyber breaches by hiring cybersecurity consultants, or transferring cyber risk by purchasing cyber insurance. It is overwhelming for SMEs to choose a method that works since they are not familiar with the cybersecurity market. Without proper cybersecurity guidance, selecting a reliable cybersecurity solution will be difficult and time-consuming, thus becoming another challenge for SMEs. Since knowing the importance and complexity of protecting an SME from a cyber-attack might be beyond the ability of the average SME, where should an SME start?

One low-cost and immediate action step is to develop a formal password policy. Passwords are one of the easiest ways for hackers to access the data that SMEs choose to put online. This is due to two things: a lack of formal policies that require password changes, as well as employees being unaware of what makes a password strong. Thus, it is also important to evaluate each password and change the ones that are too weak. Although enforcing a strong password policy is important, it is recommended not to create a password policy that is too complex, as employees may "cheat" to remember the password. "Cheating" in this case refers to actions such as writing the password down or constantly using the same password for everything. A password policy must contain a mix of letters, numbers, and symbols to ensure that it is strong, and must be changed periodically. (GFI) Additionally, when employees leave the business, steps must be taken to change passwords to ensure disgruntled employees can no longer access any valuable data.

Another important action step is to properly train all employees in cybersecurity. Many cyber breaches are the result of improper actions of employees, and it is becoming a big security threat for SMEs. In the NCSA survey, 7 in 10 SMEs don't have any Internet security policies, whether they are formal or informal, and only one-quarter of SMEs have restrictions on social media usage for employees. (NCSA) SMEs must be aware of their employee's role in cyber risk prevention and restrict their access to certain

accounts and data. A way to restrict access includes regulating employees' external equipment usage to prevent data loss and malware installation from outside media. (Maude)

Furthermore, SMEs need to monitor their network and update their IT equipment routinely when conducting their business. SMEs have a tendency to upload their data on the Internet since it is easily accessible and doing so does not require a lot of IT knowledge. To assess the SMEs cyber risk level, they must identify their critical data they have stored on the Internet. Also, in an SME, there are many different types of people who have access to critical information such as employees, clients, hired consultants, insurance companies, and other third-party businesses. It is important to monitor their access to the company's assets especially after they leave the company or finish their business with the company. Also, if the SME monitors their network all the time, it is easier to identify abnormal activities so that timely actions can be taken to prevent further damage to the company. (PwC)

It is also important to regularly conduct IT system security tests to improve cyber risk prevention. These security tests can be conducted either internally or by a third-party. Using both internal and external resources helps provide checks and balances to ensure that the SME is operating as securely as possible. It also allows a way for the SME to estimate their data or business recovery time and improve the efficiency in their recovery procedures. (PwC)

Finally, establishing a cyber risk incident response team is a great way for SMEs to be prepared in the event that a hacker does indeed breach their security system. Establishing a team provides multiple benefits. One benefit is that the stress caused by the breach, and the work required to fix the issue can be distributed throughout the team. Another benefit is that having a team, rather than an individual, means that the response time, in general, will be quicker, and the SME will be able to rectify the issue in a timely manner. This means that the SME will be limiting the amount of reputation damage suffered, and there will be a lower number of customer delays, ultimately leading to a better business experience.

After all of the above challenges and actions, SMEs will have adequate test results and data to fully understand a business's cyber risk tolerance level. The cyber risk tolerance level is a threshold that each SME sets based on how well they can protect themselves from cyber incidents. (Sung & Hanna) If a cyber incident can be resolved by the SME on its own, this means that the cyber incident is lower than the SMEs cyber risk threshold. If the SME thinks that a cyber incident will exceed their cyber risk threshold in the future, they may need to consider purchasing cyber insurance to transfer these cyber risks.

Cyber Insurance

Cyber insurance was introduced to businesses many years ago when the concept of "cyber" was first introduced in 2000. Since then, frequent cyber incidents have revealed that current cyber risk management strategies are inadequate for cyber threats nowadays. As a security option, cyber insurance can cover the types of cyber risks that exceed an SMEs cyber risk tolerance level. Many insurance companies have their general liability coverages, identity theft coverages, and ransom coverages, which incorporate some cyber insurance coverages, but the coverages are not comprehensive enough to cover all types of cyber risk. Cyber insurance for SMEs covers two parties categorized as "First-Party Coverage" and "Third-Party Coverage" and Figures 8 and 9 list these coverages.

First-Party Coverage	
Category	Description
Physical Asset Damage	Damage on IT equipment, IT systems and technology.
Business Interruption	Result from denial of services, website offline and employee down time.
State-Sponsored and Terrorists Cyber Attacks	Cyber attacks result from cyber warfare or terrorists.
Theft	Theft of data, ecnomic value of intellectual property, finished goods in provess, extortion, computing recources and deceptive fund transfer.
Business Loss and Client Loss	Data disclosure of personal and business information that result in a business losing its revenue during normal operation.
Recovery of Data and System	The cost to restore data or systems that has been damaged or destoryed.
Forensic Cost	The cost to investigate cyber incidents and notifcation expenses.
Response Cost	The cost to minimize post-incident losses.

Third-Party Coverage	
Category	Description
Bodily Injury	Mental suffering, mental injury, shock, fright or other similar terms.
Third-Party Asset Damage	Infrigement of third-party intelectual property such as designs, symbols, images and new ideas.
Privacy Liability	Loss of clients' private information and employee personal data.
Reputational Liability	Infrigement of third party company's brand through first-party's network.
Third-Party Privacy Liability	Liability relating to third-party company's information.
Regulatory Fines and Penalties	Government or state fines on inappropriate data leaking caused by cyber incidents.

Figure 8 & 9. Reproduced Courtesy of (Betterley 2016) (Marsh)

Some insurance companies offer cyber insurance, but the market for SMEs is being underutilized. Less than 3 percent of SMEs have cyber insurance whereas 40 percent of large businesses have cyber coverages. (Aon) A list of possible explanations for why the cyber insurance market for SMEs is being underutilized is described below:

- Lack of cyber risk knowledge

As seen in the perception versus reality section of this report, SMEs are unaware of the potential cyber risks that could affect their company. This means that not only are SMEs unaware that they are at risk, they are doing nothing to protect themselves from these risks. While a lack of knowledge is a contributing factor as to why cyber risk is being underutilized, lack of insurance advertising also contributes to this underutilization.

- Lack of cyber insurance marketing

SMEs are unaware they are at risk, and insurance companies have not focused on highlighting or marketing this gap. This may be due to the fact that the cyber insurance market for SMEs is a developing market, but other cybersecurity markets such as purchasing antivirus software have already grown into a

developed market. Understanding and purchasing cyber insurance may not be as easy and accessible as purchasing antivirus software for SMEs.

- ➢ Inadequate funds invested in cyber insurance

Even with proper knowledge and marketing, many SMEs either lack adequate funds to afford to take preventative measures to secure against cyber risks or do not prioritize cyber risk as a need in their budget. At this time, many SMEs do not believe that purchasing cyber insurance is a necessity.

Insurers Challenges for Providing Cyber Coverage

The key for providing cyber insurance is directly related to the business for which the policy is being created. With large businesses, cyber insurance policies can be created so that one policy may fit multiple business sectors. This is not the case when it comes to SMEs. Policies must be created in such a way that they are molded specifically to fit the needs of SMEs for each business sector. So insurance providers must customize each policy based on the uniqueness, needs, and wants of each business sector. There are many factors that play a role in creating an affordable, yet comprehensive policy and they are as follows.

- ➢ Pricing cyber insurance

Pricing is a large component in offering cyber insurance to SMEs. As noted in the perception versus reality section, SMEs do not believe that cyber risk is a necessity. There is a perception that cyber risk is not important, and that cyber insurance is a waste of money. However, we know that cyber risk is a real and growing threat, and can have a costly impact. Due to these facts, it is important to create a reasonably priced policy in order for SMEs to both afford the policy and be willing to buy it. This means that for any given policy, its premiums, deductibles, and policy limits must be adjusted accordingly to fit the needs and budget that SMEs tend to work with. So in general, SMEs on average will be paying less in premiums

and deductibles compared to large businesses, which implies that they will have relatively smaller policy limits.

- ➢ Streamlined cyber insurance underwriting process

SMEs who have poor cyber risk prevention tools and procedures may have greater cyber risk exposure. Having a proper cyber insurance underwriting process for SMEs will protect insurance companies by ensuring that cyber insurance is being priced rationally. Thus the underwriting process will have to vary by business sector, for the same reasons that cyber insurance varies by business sector.

- ➢ Tailored and distinctly defined cyber insurance coverages

Coverages for cyber insurance policies must fit SMEs needs and wants. As mentioned earlier, SMEs vary by business sector, so insurance for SMEs must also be tailored in a similar fashion. What may be an ideal cyber insurance policy for the healthcare sector might be unfit for the retail sector. Due to the variety of business sectors, the cyber policy has to address the high cyber risk concerns while mitigating the low cyber risks specific for each business sector in order to make it affordable and comprehensive.

It is known that coverages for SMEs will not include the exact same coverages that large businesses have. So it is important to break down what a basic SME policy should have. First off, the policy has to cover cyber costs that are caused not only by cyber incidents or breaches, but also costs that are associated with cyber forensic. Cyber forensic is often overlooked by many SMEs, even though cyber forensic is often required after a breach to determine the extent of the damage. Coverages should also cover cyber costs that are related to civil, criminal, and administrative fines and penalties. (Betterley) These are the costs that are typically missed, yet should be included in any given cyber insurance policy. Lastly, most cyber insurance policies should cover damage or destruction of tangible property. (Safehold) Tangible property for cyber insurance purposes must be strictly related to cyber incidents, thus eliminating overlaps with other insurance policies.

- Cyber insurance cancellation policies

For a given cyber claim for SMEs, the insurer will refund any unearned premium if the insured agrees to absolve the insurer from all obligations. Otherwise, the premium should be deemed fully earned and there is no return of premiums. This method creates both affordable and flexible cancellation policies that are needed to encourage SMEs to purchase cyber insurance with confidence. (Safehold)

Monitoring and Tracking Cyber Risk Costs

Since cyber insurance for SMEs is being underutilized by insurance companies, there are not many existing databases which monitor and track SMEs cyber risk costs. Also, due to the rapidly evolving technology and the increasing tendency for SMEs to depend on technology, such databases need to be created and updated frequently. So it is critical for insurance companies to conduct cyber risk insurance audits for SMEs so that correct and timely adjustments can be made, and this new information can be applied to current premiums and the pricing of future cyber insurance policies.

First, develop a database of all SMEs who purchase cyber insurance coverages. The database should include several underwriting characteristics of SMEs such as size, business sector, current cybersecurity policy, etc. The database should also record the frequency, severity, recurrence and type of each cyber claim that is incurred. Similar to other well-developed Property & Casualty coverages where key actuarial assumptions are supported by experience data and research, any established research center could be well-positioned to develop and manage this cyber risk tracking and monitoring process with the support of cyber insurance carriers under the sponsorship of the Casualty Actuarial Society.

Secondly, update the database frequently and write periodic reports analyzing cyber risk claims by frequency, severity, recurrence, and type. Also analyze the claims by SME size, by underwriting rating and by business sectors.

Lastly, use the data collected to develop a frequency and severity predictive model based on historical claim experience to better understand cyber insurance needs. This method will lead to a more accurate and efficient insurance policy, with will lead to reduced cyber claim costs for insurers and fairer cyber insurance premiums for SMEs.

Conclusion and Next Steps

Cyber risk is a real and growing concern for SMEs that is greatly underestimated by SME owners. This is reflected in the fact that cyber risk is seldom a component of strategic risk management for SMEs and cyber insurance is significantly underutilized by SMEs. The cost to protect against cyber risk by improving operational efficiencies and purchasing cyber insurance is a small fraction of the potential cost resulting from a cyber breach. Insurance companies that offer cyber insurance should ensure that the coverage is both affordable and comprehensive, and tailored towards the individual needs.

Cyber risk for SMEs is relatively new and the cyber risk insurance market for SMEs is not well-developed. Hence, it is important to develop a comprehensive tracking and monitoring process of cyber risk cost with data provided by insurance carriers. This will allow us to analyze cyber risk cost by various business sectors, size, and other critical factors.

About The Goldenson Center

The Janet & Mark L. Goldenson Center for Actuarial Research was established in June 2009. It is known for its leading think-tank for applied actuarial research. Donations from the Goldenson family are directed towards applied actuarial research to serve the needs of the financial services industry and to provide real-life experience to actuarial students. It is overseen by an advisory board of industry executives and key University of Connecticut academic staff.

The Authors

Director:
Dr. Jay Vadiveloo
PhD, FSA, MAAA, CFA
Jeyaraj.Vadiveloo@Uconn.edu

Faculty:
Gao Niu ----- Reached at Gao.Niu@Uconn.edu

Co-authors:
Jay Krutiak - Reached at Jay.Krutiak@Uconn.edu
Jing Guo ---- Reached at Jing.Guo@Uconn.edu
Junyi Yang - Reached at Junyi.Yang@Uconn.edu

Sponsors:
Chubb Group
CoverHound
Symantec

References

Ablon, Lillian, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky. Consumer Attitudes toward Data Breach Notifications and Loss of Personal Information. N.p.: n.p., n.d. RAND Corporation, 2016. Web.
<http://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf>

Advisen Ltd. "Cyber Liability Insurance Market Trends: Survey." (n.d.): n. pag. Oct. 2015. Web.
<http://www.advisenltd.com/wp-content/uploads/2015/10/cyber-liability-insurance-market-trends-survey-2015-10-16.pdf>

Aon. "Cyber - the Fast Moving Target." (n.d.): n. pag. 2016. Web.
<http://www.aon.com/attachments/risk-services/cyber/2016-Captive-Cyber-Survey-Interactive.pdf>.

Betterley, Richard. "Cyber/Privacy Insurance Market Survey - 2016." (n.d.): Rep. BRC, May-June 2016. Web. July-Aug. 2016.
<https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf>

Biener, Christian, Martin Eling, and Jan Wirfs. "Working Papers on Risk Management and Insurance." Insurance of Cyber Risk: An Empirical Analysis (n.d.): n. pag. Jan. 2015. Web
<http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf>

Cebula, James, and Lisa Young. "A Taxonomy of Operational Cybersecurity Risks." (n.d.): n. pag. Dec. 2010. Web.
<http://www.sei.cmu.edu/reports/10tn028.pdf>

Filkins, Barbara. "IT Security Spending Trends." SANS Institute, Feb. 2016. Web. <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>.

GFI white paper. ”Security Threats: A Guide for Small and Medium Enterprises.” Microsoft Gold Certified Partner. 2011 <https://www.gfi.com/whitepapers/Security_threats_SMEs.pdf>

Gustke, Constance. "No Business Too Small to Be Hacked." The New York Times. The New York Times, 13 Jan. 2016. Web. 01 Aug. 2016. <http://www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0>

Hartwig, Robert, and Claire Wilkinson. *CYBER RISKS: THE GROWING THREAT* (n.d.): n. pag. Insurance Information Institute (III), June 2014. Web. *Http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf*.

Herath, Hermantha, and Tejaswini Herath. "Insurance Markets and Companies: Analyses and Actuarial Computations." Copula-based Actuarial Model for Pricing Cyber-insurance Policies 2011th ser. 2.1 (n.d.): n. pag. Web. <http://www.businessperspectives.org/journals_free/imc/2011/IMC_2011_1_Herath.pdf>

KPMG. "Small Business Reputation & the Cyber Risk.": n. pag. 2016. Web. <http://www.kpmg.com/channelislands/en/about/Documents/small-business-reputation-and-the-cyber-risk.pdf>

Lopez, Jose A. "What Is Operational Risk?" *Federal Reserve Bank of San Francisco*. Federal Reserve Bank of San Francisco Search SF Fed, 25 Jan. 2002. Web. 15 Aug. 2016. <http://www.frbsf.org/economic-research/publications/economic-letter/2002/january/what-is-operational-risk/>.

Maude, Francis. *The Role of Insurance in Managing and Mitigating the Risk*. Rep. Marsh, Mar. 2015. Web. 16 Aug. 2016. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf>.

Menz, Norman. "Improving Third Party Risk Management with Cyber Threat Intelligence.": n. pag. Prevalent, Apr. 2015. Web. July-Aug. 2016. <http://www.isaca.org/chapters11/Western-New-York/Events/Documents/2015-April/CT02-3RD-Party-Cybersecurity-NMenz.pdf>

NCSA. "America's Small Businesses Must Take Online Security More Seriously.": n. pag. 2015. Web. <https://staysafeonline.org/download/datasets/4629/ncsa_small_business_infographic_final.pdf>

NCSA/Symantec. "National Small Business Study." Oct. 2012. Web. <https://staysafeonline.org/download/datasets/4389/2012_ncsa_symantec_small_business_study.pdf>

NetDiligence. "2014 Cyber Claims Study." (2014): n. pag. Web. <http://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2014-Cyber-Claims-Study.pdf>

NetDiligence/Symantec. "2015 Cyber Claims Study." (n.d.): n. pag. May 2016. Web. <http://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015.pdf>

NSBA. "2014 Year-end Economic Report.": n. pag. Feb. 2015. Web. <http://www.nsba.biz/wp-content/uploads/2015/02/Year-End-Economic-Report-2014.pdf>

NSBA. "2015 Year-end Economic Report.": n. pag. Feb. 2016. Web. <http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf>

Ponemon Institute. *2015 North America Cyber Impact Report*. Rep. Ponemon Institute, June 2015. Web. 16 Aug. 2016.

Sung, Jaimie, and Sherman Hanna. "Factors Related To Risk Tolerance." *Journal of Financial Counseling and Planning* 7 (1996): 11-19. *ProQuest*. Web. 16 Aug. 2016.

Temi Abimbola, Christine Vallaster, (2007) "Brand, organizational identity and reputation in SMEs: an overview", Qualitative Market Research: An International Journal, Vol. 10 Iss: 4, pp.341 - 348. <https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html>

Vaizey, Ed. “2015 Information Security Breaches Survey.": n. pag. PwC. 2015. Web. <https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf>

Willetts, David. "2014 Information Security Breaches Survey." 2014.1: n. pag. PwC. Web. <http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf>