# 2017 STATE OF CYBERSECURITY AMONG SMALL BUSINESSES IN NORTH AMERICA

BBB®

CYBER $3CUR1TY℠

# EXECUTIVE SUMMARY

Earning and maintaining trust in the contemporary digitalized world is only getting more complex and difficult. In particular, CEOs of large global organizations are especially concerned that cybersecurity breaches could impair public trust in their industry[1].

Cybersecurity threats are also of great concern to small business owners, since organizations of all sizes are at risk for cyberattacks. In fact, small businesses – which make up more than 97% of total businesses in North America – have a unique role in the cybersecurity ecosystem and overall national security strategies: they can be targeted by cybercriminals as gateways through the supply chain to larger corporations, many of which are in critical infrastructure sectors[2].

In keeping with its mission to advance marketplace trust for all, the Better Business Bureau (BBB) continues its ongoing research on the topic with the 2017 *State of Cybersecurity Among Small Businesses in North America*. Among this year's findings, BBB found that small business owners are becoming more and more aware of cyberthreats, continue to be concerned about cyber risks, and are taking some proactive security steps, in spite of their unique challenges in regard to cybersecurity. Additionally, they could, and would, do more to implement changes if they had the resources and knowledge about the topic.

Cybersecurity is big business; global spending on information security is expected to reach $170 billion by 2020[3]. Thus, one important issue is the effective allocation of resources to cybersecurity – i.e., how well is the money being spent[4,5]. This question is even more critical for smaller businesses: they cannot afford to make mistakes when committing to such important and potentially expensive investments and need to be as effective as possible in the allocation of resources.

Our goal with this report is to help inform small business owners of steps they can take to approach cybersecurity investments in a more effective way and to inject some (even if minor) rationale in the way these investments are allocated. We also expect to inform policymakers on how best to support small business owners in tackling cybersecurity challenges.

It is time to focus on comprehensive cybersecurity solutions that are customized for the needs and constraints of smaller businesses. This report aims to educate and bring awareness to the topic of cybersecurity for small businesses by exploring the real and perceived risks of cyberattacks, as well as best practices for protecting against these types of security threats. We hope it serves as a step forward in advancing cybersecurity in the marketplace.

[1] https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2017/gx/trust.html

[2] https://www.dhs.gov/critical-infrastructure-sectors

[3] https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in 2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#258d844a30d6

[4] https://www.is.uni-muenster.de/security/publications/Boehme2010_SecurityInvestment-IWSEC.pdf

[5] https://file.scirp.org/pdf/JIS_2016032315382494.pdf

# INTRODUCTION

In a world increasingly dependent on digital technology, and with supply chains becoming more interconnected, and malevolent actors more sophisticated, cybersecurity has become a critical management issue.

In keeping with BBB's mission to advance marketplace trust for all, the idea behind *The State of Cybersecurity Among Small Businesses in North America* was born in 2016. In August 2017, BBB furthered its ongoing research with a poll of 2,000 consumers and a survey of about 1,100 businesses in North America. The sample was selected from a panel of business owners and from BBB Accredited Businesses which were recruited via the internet using a custom email invitation with a live link to a survey. The margin of error was approximately 3%, with a 95% confidence interval. Figure 1 shows the profile of the respondents.

The goal of the research was to collect information on the state of cybersecurity among small businesses, understand cybersecurity awareness and risks, and uncover the challenges faced by smaller businesses that could lead to better cybersecurity practices. The primary objectives of this report are to advise our community of trusted businesses and the marketplace at large; advance conversation around cybersecurity effectiveness; dispel common misperceptions; show that cybersecurity could eventually become a driver for consumers' purchasing decisions; and inform cybersecurity policy, research, and education and awareness efforts.

FIGURE 1

## PROFILE OF RESPONDENTS

| | | |
|---|---|---|
| 71.4% | 28.5% | 0.1% |

### AGE RANGE

| 18-34 | 35-54 | 55+ |
|---|---|---|
| 21% | 45% | 34% |

### GENDER

| | |
|---|---|
| 55% | 45% |

### FULL TIME EMLPOYEES

| 0-5 | 6-10 | 11-49 | 50-249 | 250+ |
|---|---|---|---|---|
| 54% | 13% | 18% | 9% | 6% |

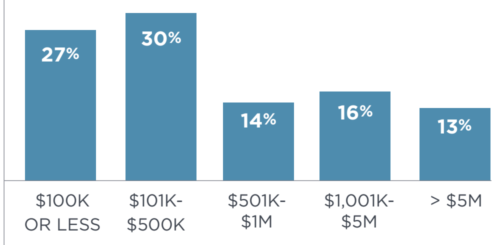
### POSITION/TITLE

| CEO/OWNER | VP/DIRECTOR | MANAGER | OTHER |
|---|---|---|---|
| 66% | 14% | 14% | 6% |

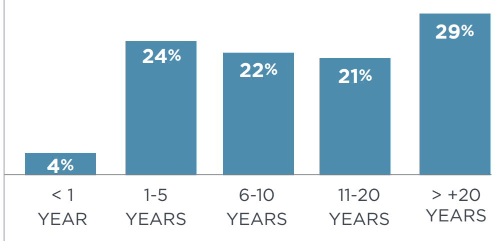
### TYPE OF BUSINESS

| | |
|---|---|
| 14% | CONSTRUCTION & HOME SERVICES |
| 12% | SERVICES |
| 10% | PROFESSIONAL SERVICES |
| 8% | RETAIL |
| 8% | FINANCE & INSURANCE |
| 7% | HEALTH CARE AND SOCIAL ASSISTANCE |
| 6% | TECHNOLOGY |
| 5% | REAL ESTATE |
| 4% | AUTOMOTIVE |
| 4% | MANUFACTURING |
| 4% | ACCOMMODATION & FOOD SERVICE |
| 3% | WHOLESALE |
| 2% | TRANSPORTATION & WAREHOUSING |
| 13% | OTHER |

### REVENUE (IN US DOLLARS)



### TENURE



### BBB ACCREDITED BUSINESS (AB) STATUS

| AB | NON-AB |
|---|---|
| 67% | 33% |

# CYBERSECURITY AWARENESS, UNDERSTANDING, AND PRACTICES

Cybersecurity – the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access – is a popular topic in government and corporate circles, and is a growing concern for smaller businesses.

Cybersecurity awareness among smaller businesses has come a long way in the last few years with the increasing prominence of the problem.[6] Thus, not surprisingly, 76% of businesses in our study are aware of the risk of phishing and about 93% of BBB Accredited Businesses have heard of at least one of the most prevalent risks to cybersecurity described in Figure 2 below.

FIGURE 2

| HAVE YOU HEARD OF ANY OF THE FOLLOWING RISKS TO YOUR ORGANIZATION'S CYBERSECURITY? PLEASE SELECT ALL THAT APPLY. | AB STATUS | | |
|---|---|---|---|
| | AB | NON-AB | OVERALL |
| **RANSOMWARE:** Scammers breach the operating system and download a type of malicious software designed to block access to a computer system or hold data hostage until a sum of money is paid. | 65% | 67% | 66% |
| **PHISHING:** Communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the business into providing sensitive information or passwords. | 76% | 76% | 76% |
| **POINT-OF-SALE MALWARE:** Specialized malware loaded onto point-of-sale devices that remotely captures data from each card swiped at that cash register. | 57% | 42% | 52% |
| **KEYLOGGERS:** Hardware or software that captures each keystroke on a device and makes it available to an attacker. | 45% | 37% | 43% |
| **TECH SUPPORT PHONE SCAM:** Scammers pose as a security monitoring service that has (falsely) detected a virus on your computer. Often, they then charge you to install software to clean it up. This software actually gives them remote access to your computer. | 66% | 62% | 65% |
| **REMOTE ACCESS TROJAN or RAT**: Malware that connects to an attacker's server and provides complete access to the infected machine including keyboard, screen, webcam, and files. | 57% | 54% | 56% |
| **N/A:** I have not heard of any of these risks | 7% | 12% | 8% |

[6] https://www.zurich.com/en/media/news-releases/2016/2016-1123-01

FIGURE 3

| **QUESTION: BASED ON YOUR CURRENT UNDERSTANDING OF CYBERSECURITY, RATE THE FOLLOWING STATEMENTS AS TRUE OR FALSE.** | **% OF CORRECT RESPONSES** |
|---|---|
| Small businesses are safe from cyberattack(s). **FALSE** | 87% |
| When making an investment in cybersecurity, you should consider a) the value of the data, b) the probability it can be breached, AND c) the effectiveness or ”bang for your buck” that the new control provides. **TRUE** | 85% |
| Three quarters of breaches in the hotel and restaurant industry involved point-of-sale systems. **TRUE** | 80% |
| Over 90% of successful cyberattacks start as phishing emails. **TRUE** | 79% |
| The cybersecurity industry is making progress towards defending against ransomware. **TRUE** | 78% |
| If stolen credentials resulted in a substantial loss from your business banking accounts, the bank would be responsible to cover them. **FALSE** | 50% |
| Over half of successful data breaches involved organized crime groups. **TRUE** | 48% |
| There is a limit beyond which investing in cybersecurity is not worth it. **TRUE** | 42% |
| The first thing to do if a block of data was stolen from your business, such as your customer information, is to notify those affected. **FALSE** | 20% |
| The most cost effective approach to cybersecurity is to protect the information that is most vulnerable to attack. **FALSE** | 17% |

In order to assess understanding of cybersecurity, we created a quiz and asked respondents to judge 10 statements as either true or false. The average score was below 60%, which means that, in spite of respondents' general awareness of cybersecurity risks, there are still opportunities to better educate smaller businesses on the topic and dispel some cybersecurity myths. In particular, it is important to educate small business owners around cybersecurity investment and cost effectiveness. On the investment side, 83% of respondents want to protect their most vulnerable data. While this is often the correct approach, many times the value of the data does not justify the expense. On the cost-effectiveness side, only 42% believe that there is a limit to cybersecurity spending. Per the Gordon and Loeb Framework[7] to Assess Cost Effectiveness of Cybersecurity – which we will explain in greater detail later in this report – there is a point where a dollar invested in cybersecurity results in less than a dollar's worth of protection.

A stubborn concern, with only about 20% correct responses, is around what to do first in the event of a data breach. Even though immediately notifying those affected is a responsible and ethical approach, breach notification is a complex issue that varies by state and could cause harm for the business if done incorrectly. The reporting obligation can be difficult to understand for any one state, and 48 US states and three Canadian provinces have reporting laws – all different – in addition to federal laws. Also, the law that applies depends on location of customers, not the business, so more than one law may apply if customers are in several areas[8].

Ideally, all businesses should put a plan in place before a breach occurs as part of advanced incident response planning. Consulting and following that plan should be the first thing to do if data is stolen from the business. Notifying those affected will be early in that plan, but consulting your legal counsel usually comes first.

[7] Dr. Lawrence A. Gordon is the EY Alumni Professor of Managerial Accounting and Information Assurance at the University of Maryland's Robert H. Smith School of Business. Dr. Martin Loeb is a professor of Accounting and Information Assurance and a Deloitte & Touche Faculty Fellow in the Robert H. Smith School of Business at the University of Maryland, College Park.

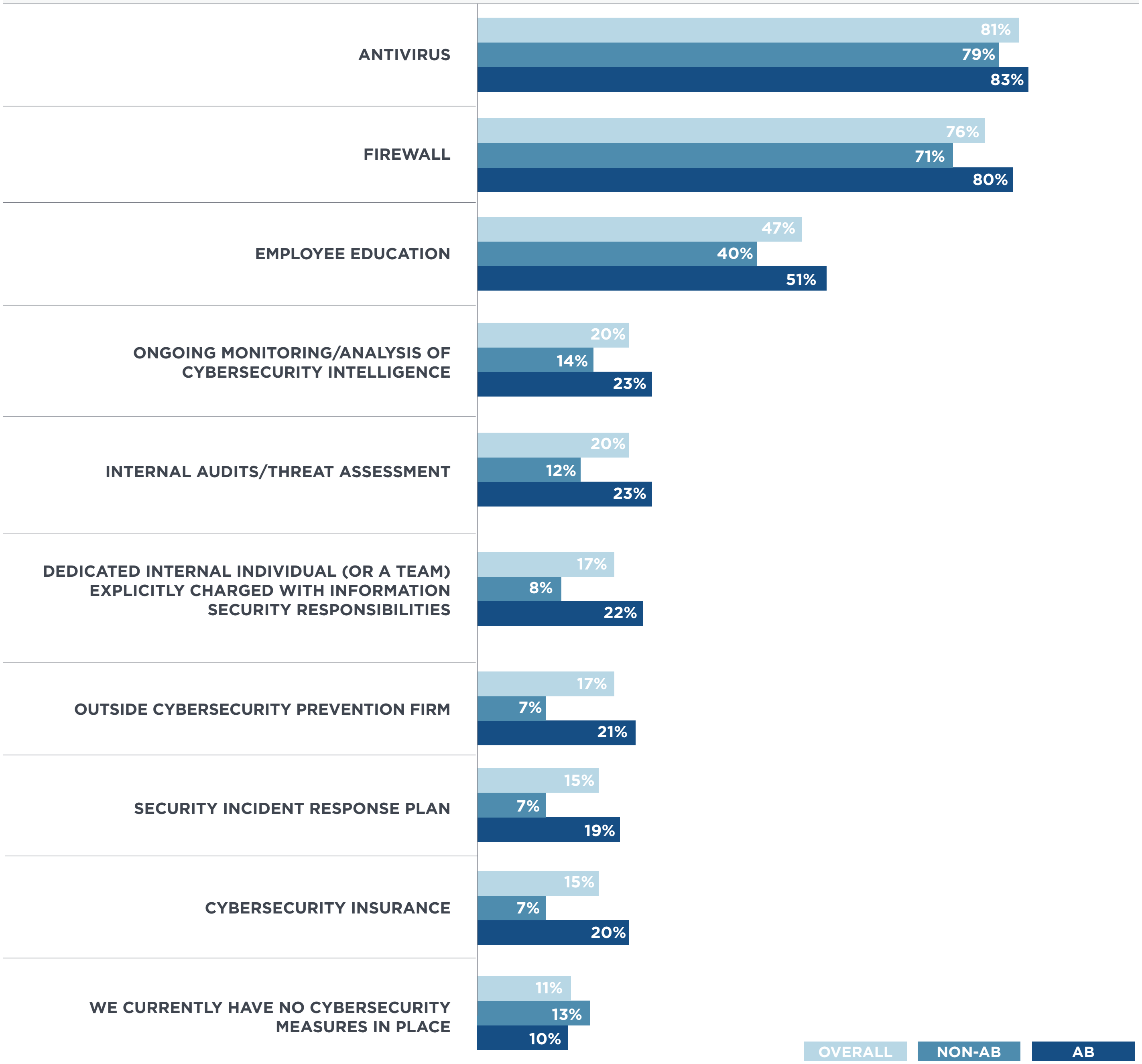
[8] The National Conference of State Legislatures provides a good summary of US laws at www.ncsl.org. An overview of Canadian legislation can be found at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

Fortunately, about nine out of ten businesses reported they have some cybersecurity measures in place, with the most common ones being: 1) antivirus; 2) firewall; and 3) employee education. BBB Accredited Businesses are almost three times as likely to include cybersecurity insurance. The financial risk of cybersecurity incidents can be transferred to insurance companies, a move that makes sense when the insurance cost is less than providing additional cost-effective protections.[9] In our study, approximately 15% of businesses had cybersecurity insurance in place to cover primarily:

**Personally identifiable information (81%); Payment card data (78%); and Incident response (54%).**

FIGURE 4

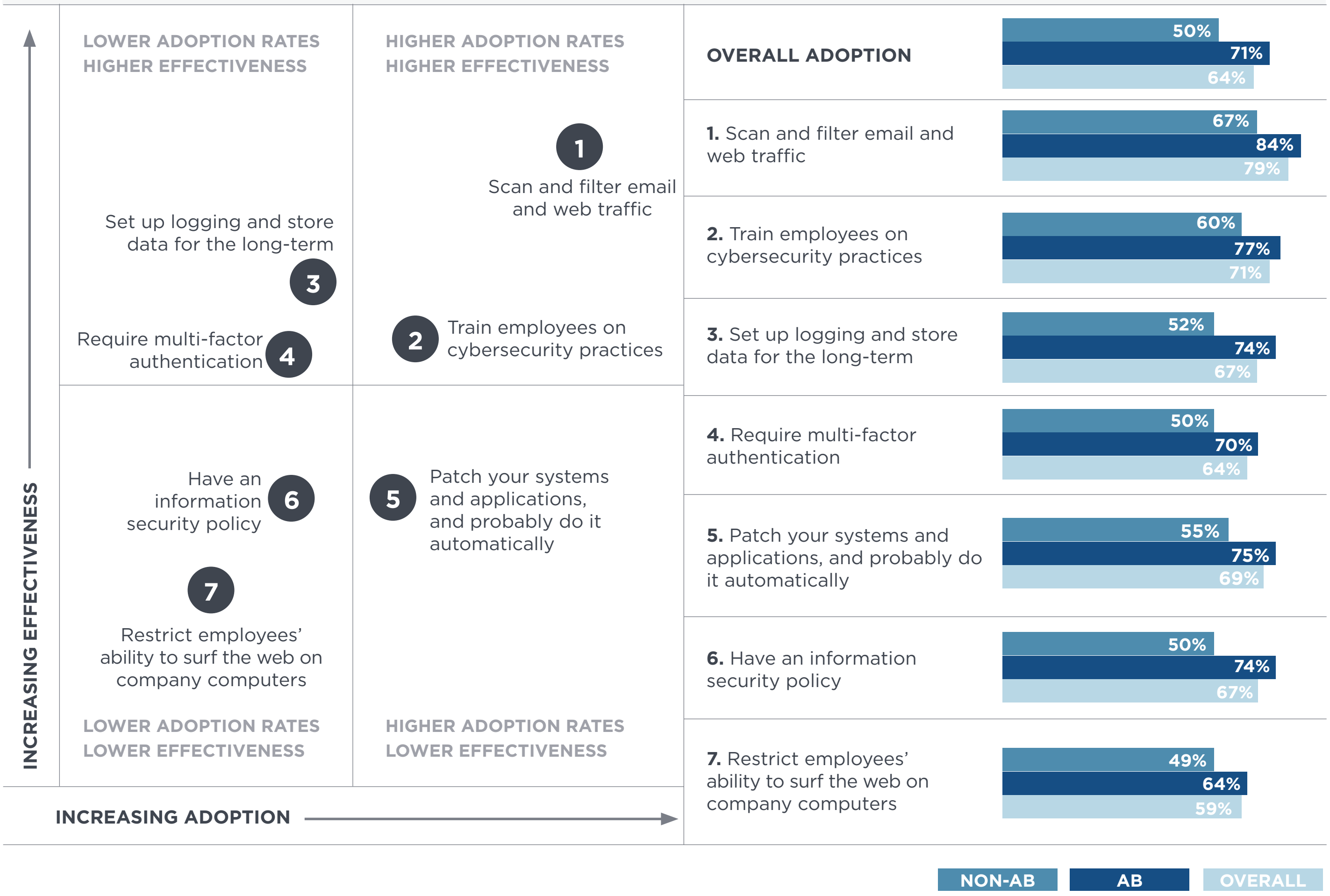
QUESTION: WHAT CYBERSECURITY MEASURES DO YOU HAVE IN PLACE TO SAFEGUARD YOUR BUSINESS? SELECT ALL THAT APPLY.



[9] https://www.is.uni-muenster.de/security/publications/Boehme2010_SecurityInvestment-IWSEC.pdf

FIGURE 5

QUESTION: FROM THE FOLLOWING CYBERSECURITY CONTROLS, PLEASE DESCRIBE HOW MUCH HAVE YOU IMPLEMENTED EACH IN YOUR ORGANIZATION AND HOW EFFECTIVE - IN TERMS OF SECURITY RESULTS - YOU BELIEVE THEM TO BE?



Since measuring cybersecurity effectiveness is complex and extremely difficult, some organizations adopt an industry standard or "best practices" approach, which seems to provide managers a feeling of some level of safety[10]. According to research from the Internet Security Alliance, there are seven basic cybersecurity controls that represent a unanimous consensus around what businesses should do.[11] Figure 5 shows a matrix with the degree of adoption of each of these controls, as well as the perceived effectiveness of each – in terms of security results – as compared with their reported averages.

The top controls (i.e., above average in terms of adoption and perceived effectiveness) are: 1) scanning and filtering email and web traffic, and 2) training employees on cybersecurity practices. Also higher than average on perceived effectiveness, but with an opportunity to grow adoption, are: 3) setting up logging and storing data for the long-term, and 4) requiring multi-factor authentication.

The BBB Accredited Businesses in our sample were apparently more likely than non-Accredited Businesses to have some type of cybersecurity control in place, even after controlling for firmographics such as similar organizational sizes (i.e., number of full time employees) and revenue profiles (Figure 5).

[10] Managing Cyber-Security Resources: A Cost-Benefit Analysis – Laurence A. Gordon and Martin P. Loeb

[11] https://isalliance.org/seven-basic-cybersecurity-measures-as-revealed-by-wisdom-of-the-crowd/

# CYBERSECURITY FRAMEWORKS

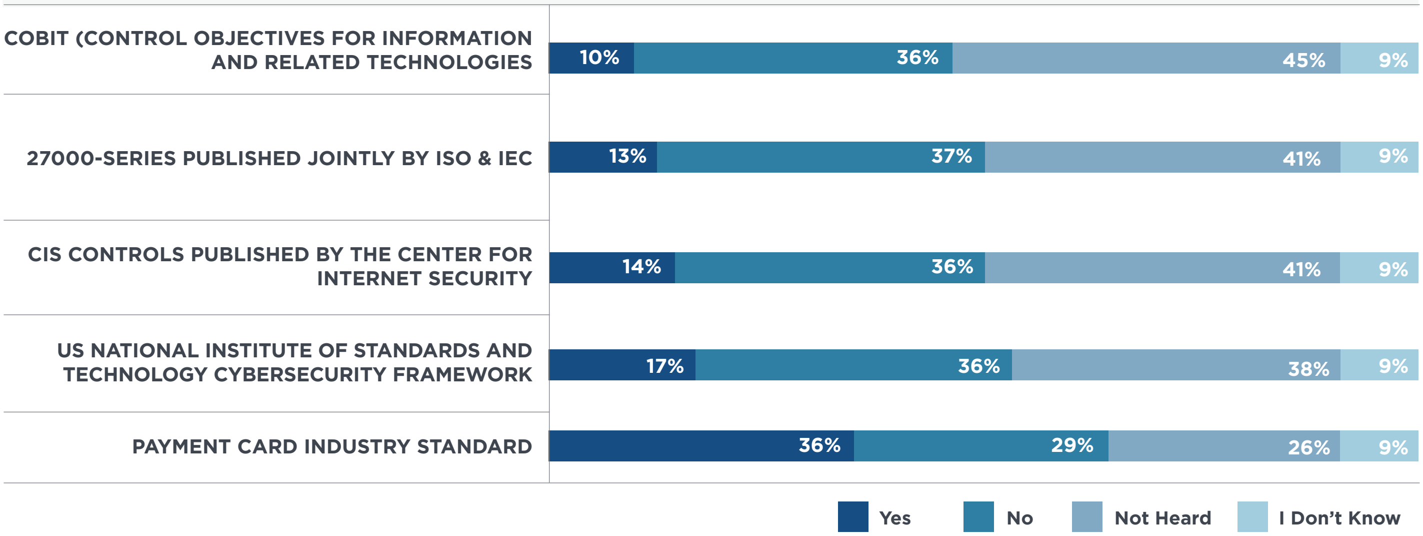
An information security framework is a “blueprint” that helps manage risks and reduces vulnerabilities in cybersecurity. It consists of a series of processes that an organization uses to define procedures and policies for the implementation and ongoing management of cybersecurity controls.[12]

The Payment Card Industry Standard and the US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) are the two most highly adopted cybersecurity frameworks (Figure 6) among our respondents. Cybersecurity frameworks are adopted voluntarily by organizations and they are more familiar to larger businesses than to small ones. For example, while approximately one out of ten organizations with zero to ten employees has adopted NIST CSF, about one out of two organizations with 250 or more employees has done the same.

The primary reasons smaller businesses chose to adopt a cybersecurity framework is a perception of being relatively better protected/safe/secure, and peace of mind. The key factors that led to the adoption of NIST CSF, in particular, are shown in Figure 7 below. They are related to its usefulness to inform cybersecurity decision-making (i.e., it is likely that the frameworks are used as a proxy to inform cybersecurity effectiveness), liability concerns (i.e., risk mitigation), and consistent risk management communication.

FIGURE 6

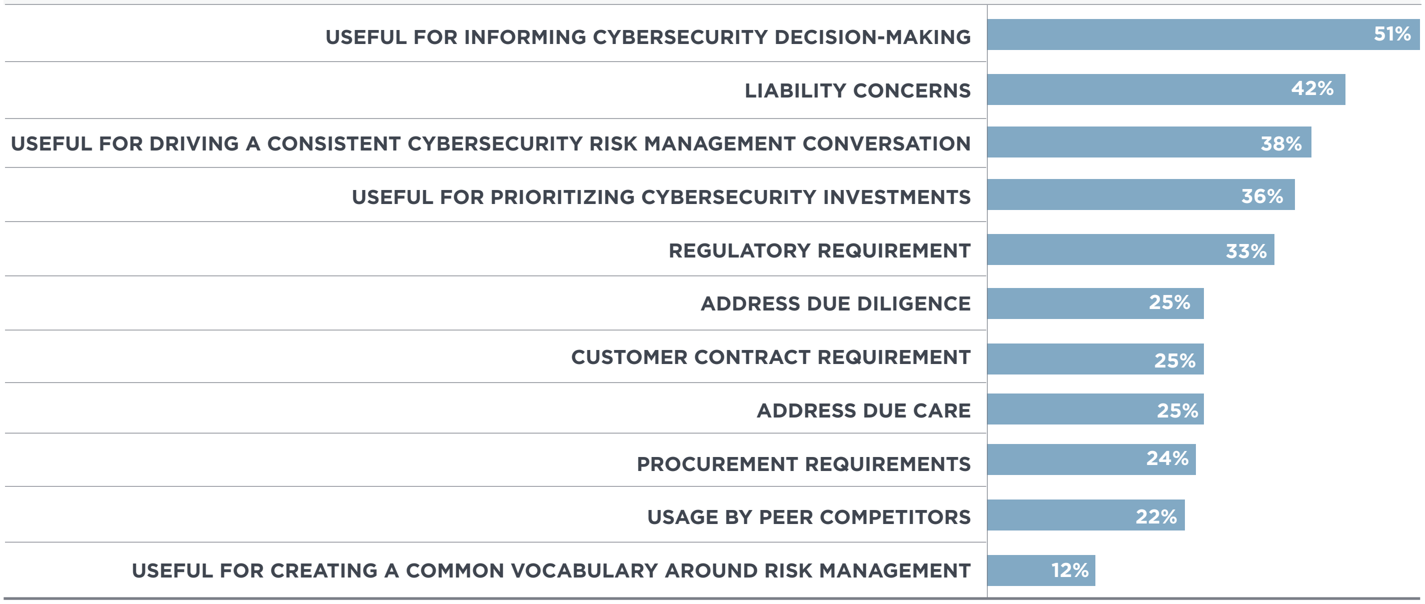
QUESTION: HAVE YOU ADOPTED ANY OF THE FOLLOWING CYBERSECURITY FRAMEWORKS?



[12] http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

FIGURE 7

QUESTION: WHAT FACTORS LED YOUR ORGANIZATION TO DECIDE TO USE THE NIST CYBERSECURITY FRAMEWORK?



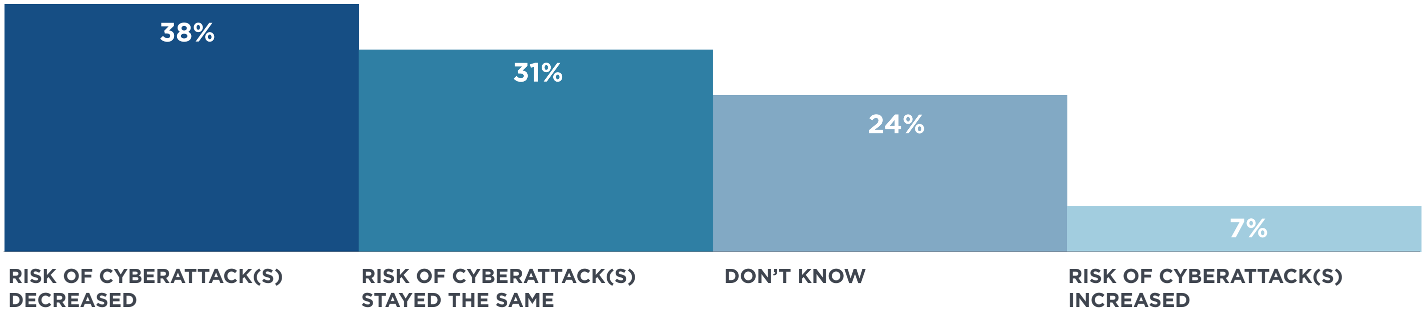
Overall, the perceived value of adopting a cybersecurity framework is positive, with approximately two out of five organizations that have adopted at least one of the studied frameworks inferring a decrease in risk (see Figure 8 below). It is important to highlight that about one out of four organizations could not tell how (if at all) the risk changed with the implementation of the cybersecurity framework.

This fact could be related to the complexity of performance measures that gauge the effectiveness of the adoption of a cybersecurity framework and/or of any other cybersecurity efforts.

Another area that businesses need to consider is whether they will be required to adopt the NIST Cybersecurity Framework. One quarter of respondents who have adopted the NIST Cybersecurity Framework report that doing so was a procurement or contract requirement. One third reported it as a regulatory requirement. It is becoming clear that, despite the fact that the NIST Cybersecurity Framework document, as well as the Presidential Executive Order that initiated it, claim that this is a voluntary framework, it is, in effect, becoming mandatory for participation in some markets.

FIGURE 8

QUESTION: HOW HAS YOUR ORGANIZATION'S RISK OF CYBERATTACKS CHANGED (IF AT ALL) WITH THE ADOPTION OF THE CYBERSECURITY FRAMEWORK?

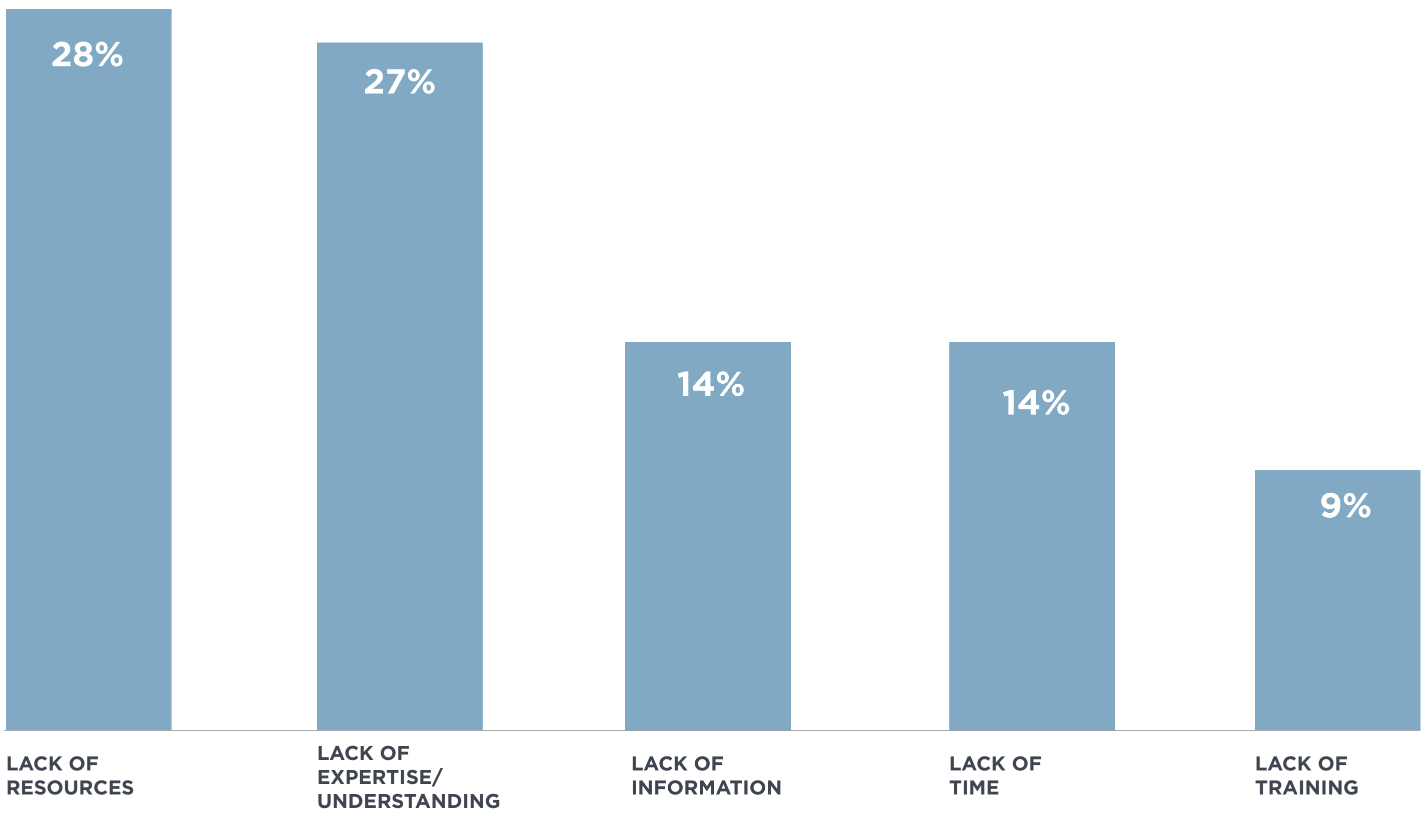


# WHAT COULD HELP SMALL BUSINESSES DO MORE?

Cybersecurity is often perceived as more costly than smaller businesses can afford; thus, cost and the organization's lack of resources is the number one challenge these businesses face in adopting cybersecurity practices (see Figure 9 below).

FIGURE 9

QUESTION: WHAT IS THE TOP FACTOR THAT HINDERS YOUR ORGANIZATION'S ABILITY TO ADVANCE CYBERSECURITY EFFORTS?



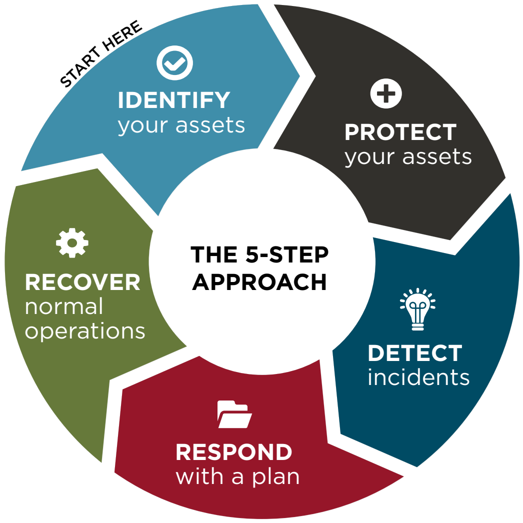
An overall lack of expertise/understanding/knowledge is another important factor. Therefore, any eventual policy solution to help small business should ideally include a knowledge-building approach.

Smaller businesses look for their cybersecurity information primarily online and via Google searches, word of mouth, IT person/company/provider, consultants/experts, and the news media. While most of the learning around cybersecurity is on the job, a few small businesses also stated that they build their knowledge in more formal training and seminars.

BBB *5 Steps to Better Business Cybersecurity* training could be an option for them to consider (see Figure 10 below). Smaller businesses are mostly interested in receiving more information about: ransomware, email authentication, encryption, and cybersecurity frameworks (see Figure 11 below).

FIGURE 10

**BBB 5 STEPS TO BETTER BUSINESS CYBERSECURITY TRAINING**[13]



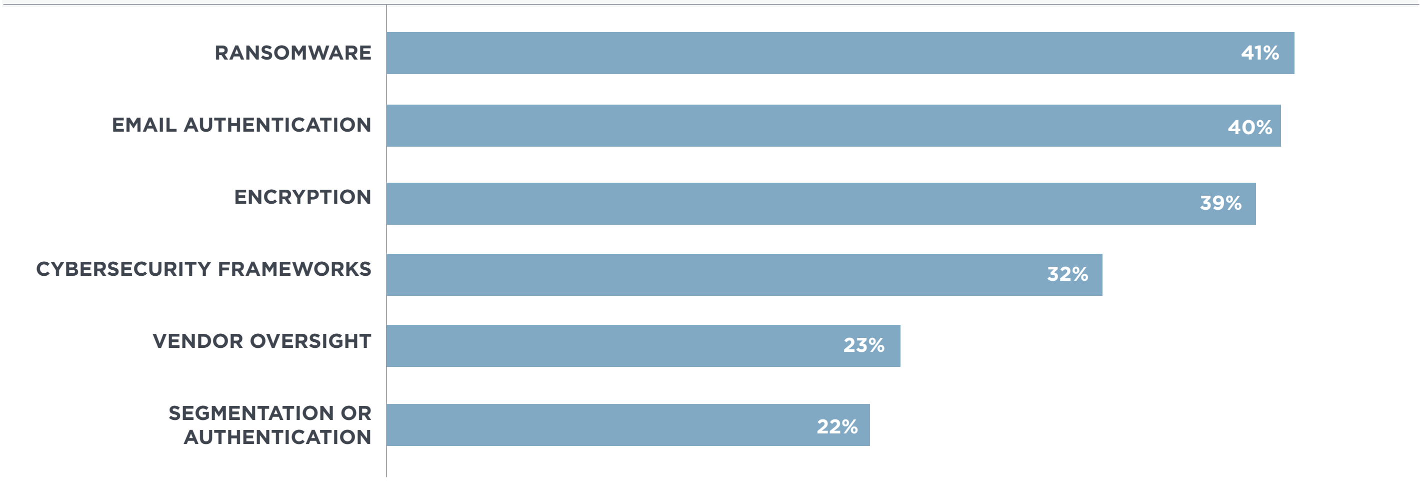
**BBB 5 STEPS TO BETTER BUSINESS CYBERSECURITY**

5 Steps to Better Business Cybersecurity, based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, represents an approach that applies to the specifics of businesses, helping them understand a process to identify and protect vital data and technology assets, and teaching them how to detect, respond to and recover from a cybersecurity incident.

bbb.org/council/for-businesses/cybersecurity/the-5-step-approach

FIGURE 11

**QUESTION: WHICH ISSUES ARE YOU MOST INTERESTED IN GETTING INFORMATION ABOUT? SELECT ALL THAT APPLY.**



[13] https://www.bbb.org/council/for-businesses/cybersecurity/the-5-step-approach

# WHAT IS THE RISK OF CYBER BREACHES?

Assessing cybersecurity risks is a function of probability of occurrence of a cyber breach and the potential loss due to such a breach. The ability to remain profitable in the event of a major data loss is the ultimate measure of successful cybersecurity planning.

Ransomware is a cyberattack that could result in such a permanent loss of data.  A far more likely event with the same data loss is a disk failure. We found that only 35% of businesses – as compared to 46% in 2016 – could remain profitable for more than three months if they permanently lost access to essential data (Figure 12). More than half would be unprofitable in under a month.  Clearly this could be an existential threat to many businesses.

FIGURE 12

QUESTION: HOW LONG COULD YOUR BUSINESS REMAIN PROFITABLE IF YOU PERMANENTLY LOST ACCESS TO ESSENTIAL DATA?

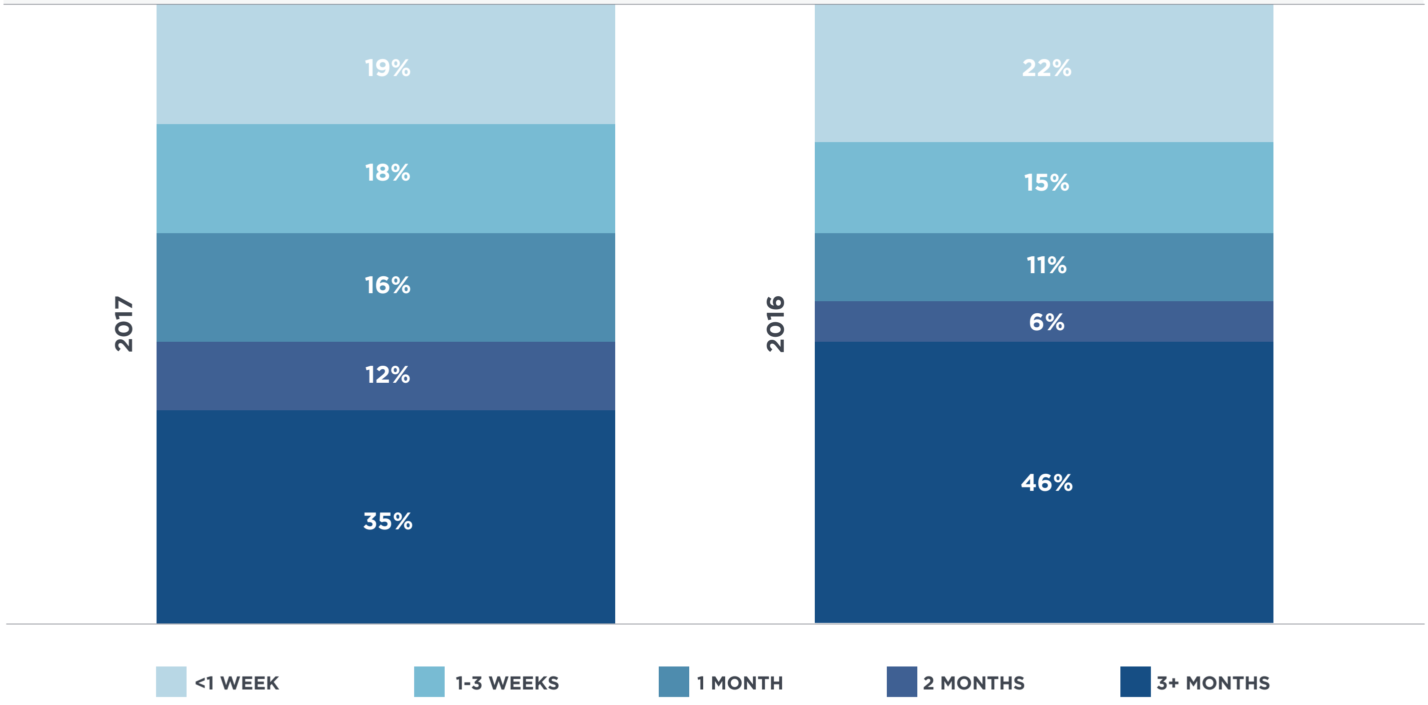
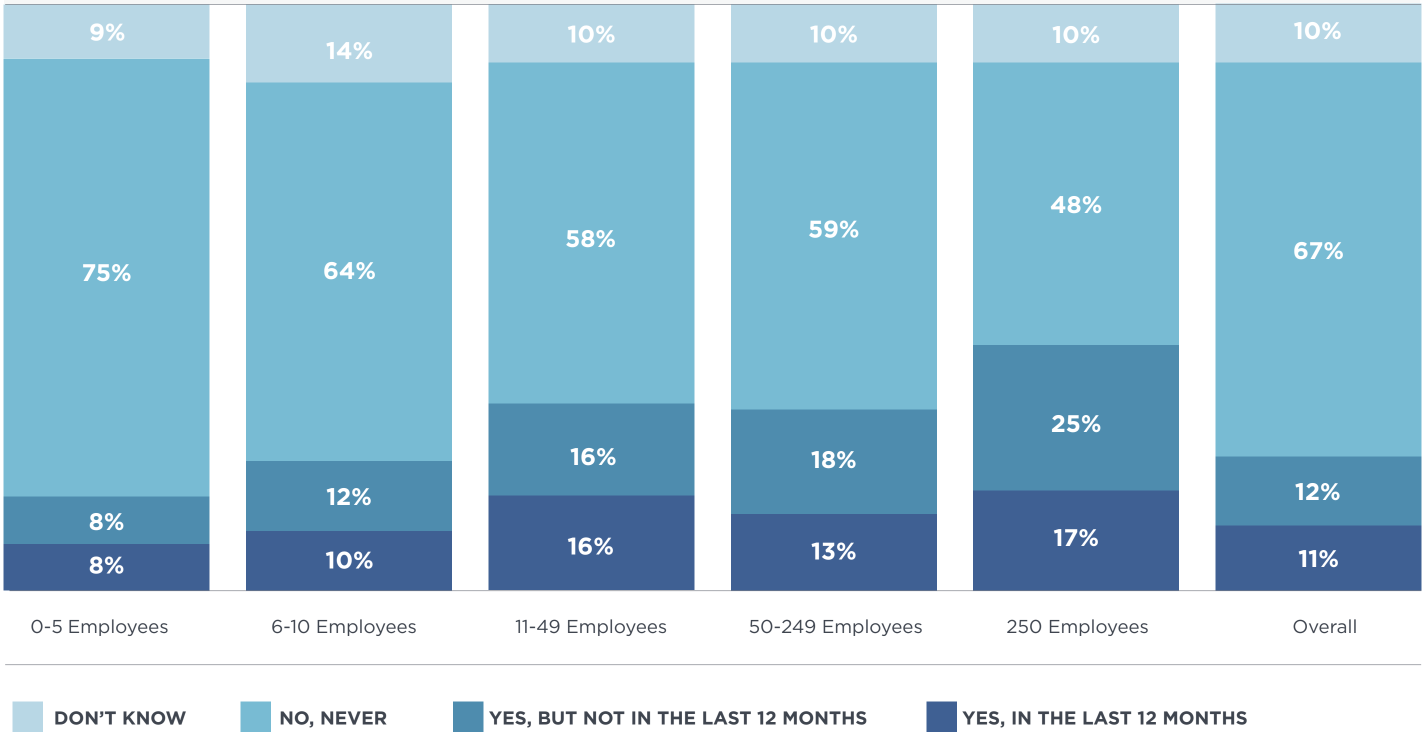


FIGURE 13

**QUESTION: HAS YOUR BUSINESS BEEN THE TARGET OF A CYBERATTACK?**



We also looked into the risk of becoming a target and losing money to a cyberattack. More than one out of five businesses reported it has been the target of a cyberattack, and approximately one out of ten reported being a target in the last 12 months. The larger the business – in terms of number of full time employees – the more likely the business was to report having been a target of a cyberattack (Figure 13).

One possible reason for larger businesses reporting higher rates of intrusion is phishing. The risk that an organization will be successfully attacked through email is directly proportional to the number of employees. One report found that over 90% of successful data breaches started with a phishing attack[14]. Only one employee needs to click on a bad link in an email or open an infected attachment for an attack to get in the door of a business.

Another possible explanation for this discrepancy is that smaller businesses may be unaware that they have been attacked. It is important to highlight that about 10% of respondents could not tell if they had been a target of a cyberattack. One reason is that many attacks have become much stealthier in recent years. Attackers can be in a system for months, sometimes years, before detection. One vendor reports that the global average to detect a cyber intrusion was 146 days[15].

Detection can be complex and expensive. It is much more likely that a larger organization has made the investment to detect such attacks – called Advanced Persistent Threats (APT). The cybersecurity industry is working to reduce the amount of time attackers are in the system before they are discovered (dwell time), and BBB is advocating for simple and lightweight detection tools for small businesses.

[14] http://www.techadvisors.us/news/article/91-of-cyberattacks-start-with-a-phishing-email

[15] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf

About 36% of the businesses that reported being a target of a cyberattack ended up losing money. And approximately 4% of the businesses overall reported having lost money to a cyberattack in the last 12 months. The overall annual average loss for smaller businesses from these cyberattacks is estimated to be US$79,841; with a median loss of US$2,000 and a maximum total loss of US$1 million.[16] The businesses estimated that their likelihood of losing money to a cyberattack in the next 12 months would increase as compared to their past risk, and approximately 16% of them expect to lose money to a cyberattack in the next 12 months.

Passwords or other authentication data, payment data, and software-based products or other copyrighted materials were the top sets of data affected (Figure 14). Figure 15 features a few of the stories from businesses that lost money to a cyberattack, in their own words, with their thoughts on why they think the cyberattack was not prevented. In one of the accounts, the respondent did not even want to talk about the incident – highlighting the fact that cybersecurity loses can be intangible and emotional, beyond merely what can be measured in monetary form.

By a wide margin, the data set affected most often was passwords and other authentication data. This reality is a major driver in recent campaigns to move from password to stronger forms of authentication.

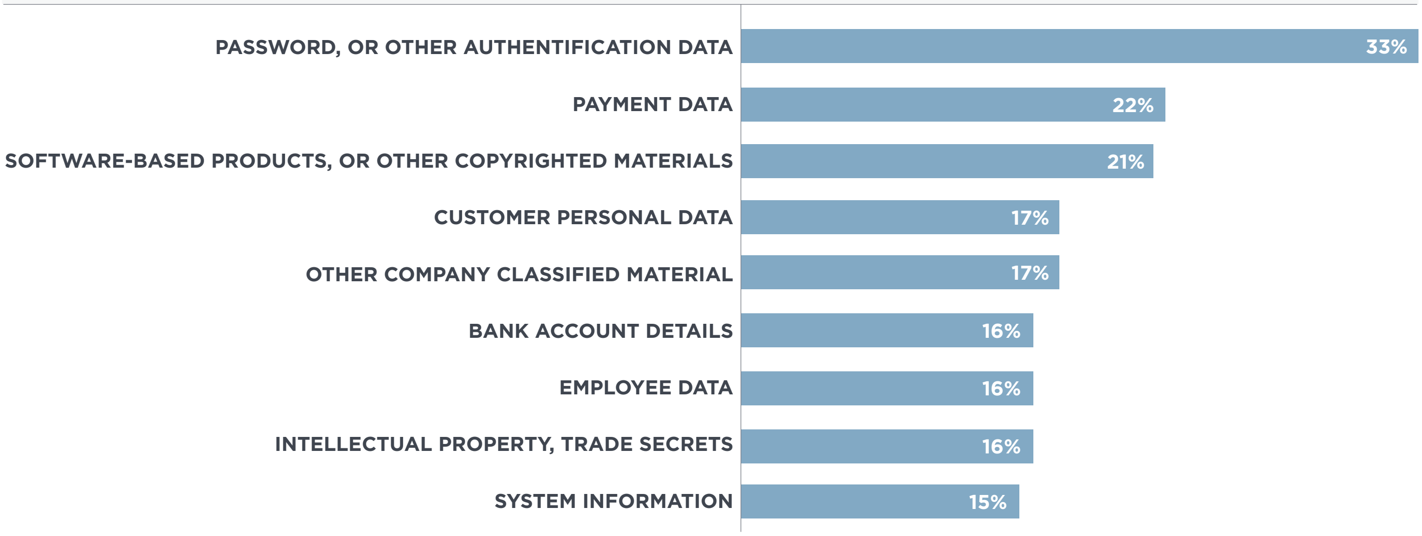
Authentication is a means of proving to a system that you are who you say you are. For example, when John presents his user name, John is stating who he is. The password proves that this is really John because only John knows the secret password.

This system works as long as passwords are hard to steal or guess. Unfortunately, there are more scams to get a user to reveal their password then would be useful to discuss here. More importantly, the bigger problem by far is that we humans are terrible about using strong passwords. In addition, we reuse them. In one analysis of passwords found in data breaches, 90% of the accounts were secured using only 1,000 different passwords[17] – and they are terrible passwords. Number one is “password.” Number two is “123456.” Only one in the top 100 passwords has a mix of numbers and letters – and it is “abc123.”

The short story is that, despite all the rhetoric about creating strong passwords, the vast majority of people use passwords that are trivial to guess. What is needed is a method of authentication that is as easy to use as a password, and, at the same time, makes it much more difficult for a bad actor to use if they guess or steal it. One approach, called stronger single-factor authentication, is to replace the password with something complex that is still easy to use; for example, fingerprint readers, retinal scans or facial recognition.

FIGURE 14

**QUESTION: WHEN YOU WERE A VICTIM OF A CYBERATTACK, PLEASE IDENTIFY WHICH SETS OF DATA WERE AFFECTED? SELECT ALL THAT APPLY.**



[16] limitations apply due to self-reported information.

[17] http://www.passwordrandom.com/most-popular-passwords

FIGURE 15

**QUESTION: PLEASE DESCRIBE A TIME (IF ANY) WHEN YOUR BUSINESS LOST MONEY TO A CYBERATTACK. WHY DO YOU THINK THE CYBERATTACK WAS NOT PREVENTED?**

*"An email was sent from a banking institution which was opened and a ransom note was given. Shut down all my computer systems and I lost all data."*

*"I lost money to a cyberattack due to a corrupt employee who stole my information."*

*"My business debit card was utilized in different states. This information could have been attained through online payments for vendors we utilize."*

*"We lost money in time, effort, and information on a limited scale. The attack was not prevented because of (1) user training and awareness, and (2) poor file location security practices."*

*"We lost $10,000 due to a cyberattack on our mainframe which a hacker was able to access financial data."*

*"Virus that wiped out hard drive after hard drive; eventually became obvious the problem was in files and backups. No virus scanners could locate it or remove. Had to replace ALL COMPUTERS and everything with USB port that plugged into, plus throw out all files and start again."*

*"Website hacked. No one responsible for updating security."*

*"We had a malfunction of our servers and the antivirus was out at the time."*

*"My bank accounts have been compromised and I was informed that the bank was encrypted to prevent any issues. They didn't have multi-level authentication or proper security measures in place."*

*"Lack of education and our antivirus not catching the virus."*

*"My potential clients were making appointments on our company website and they were getting an email from an outside company without my knowledge."*

*"Couple of times; I don't want to talk about it."*

These are very difficult for an attacker to guess or steal remotely. However, these measures introduce other challenges that need to be addressed, such as privacy issues around where and how biometric data will be stored. If an attacker discovers a password, it is a simple matter to change it, but if they obtain a copy of biometric data, the harm is potentially much greater.

Two-factor authentication addresses the problem by requiring two different forms of identity proof. This works because it is very difficult for an attacker to steal or guess both items. Many systems ask for a password and then send a code by text or email to the user. An attacker would both need to know the password and have access to the user's email or text to log into the account.

# IS IT GOOD FOR SMALL BUSINESSES TO BE CYBER SECURE?

To better understand whether it is good (or not) for smaller businesses to be cyber secure, we explored: a) the attributes that are most valued by businesses to inform their purchasing decisions, b) businesses' and consumers' perceptions of the importance of a vendor's cybersecurity approach in their purchasing decisions, and c) a few aspects of effectiveness and cost effectiveness of cybersecurity.

About 73% of businesses considered a potential vendor's approach to cybersecurity to be important or very important (see Figure 16). This is particularly true when selecting IT vendors (see Figure 17). Moreover, more than half of both consumers and businesses feel that it is important or very important for businesses to take the protection of their information seriously (see Figure 18).

FIGURE 16

QUESTION: HOW IMPORTANT ARE EACH OF THE FOLLOWING VENDOR ATTRIBUTES ON YOUR PURCHASING DECISIONS?

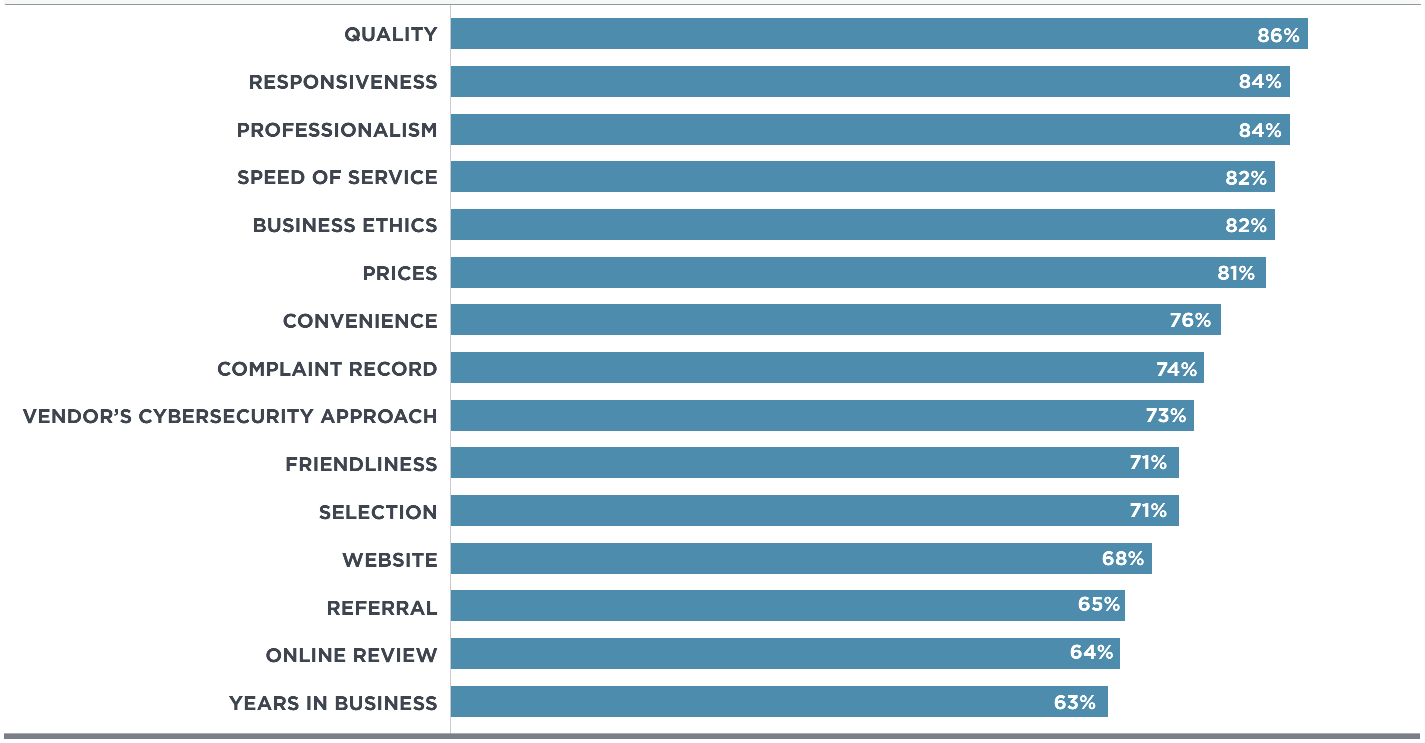


FIGURE 17

QUESTION TO BUSINESSES: HOW IMPORTANT IS THE VENDOR'S APPROACH TO CYBERSECURITY IN YOUR PURCHASING DECISION?

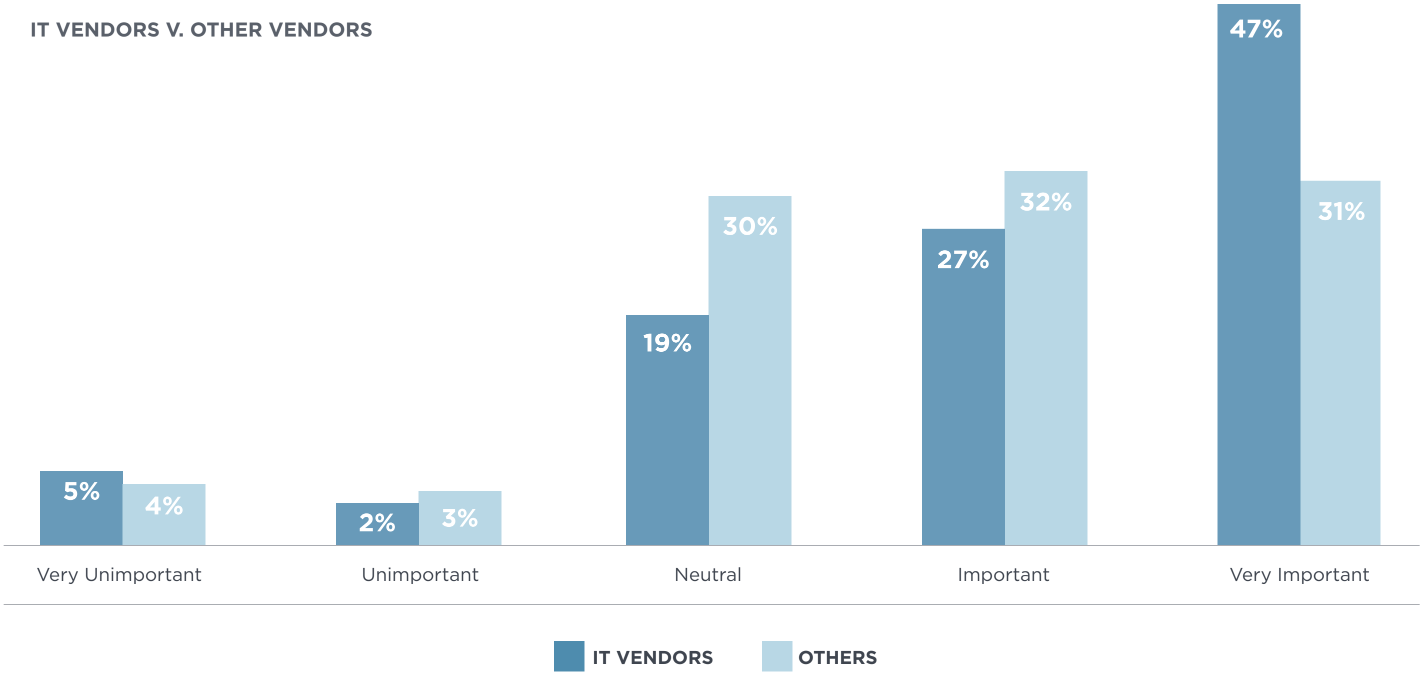


FIGURE 18

QUESTION TO BUSINESSES AND CONSUMERS: IMPORTANCE OF VENDOR'S APPROACH TO CYBERSECURITY

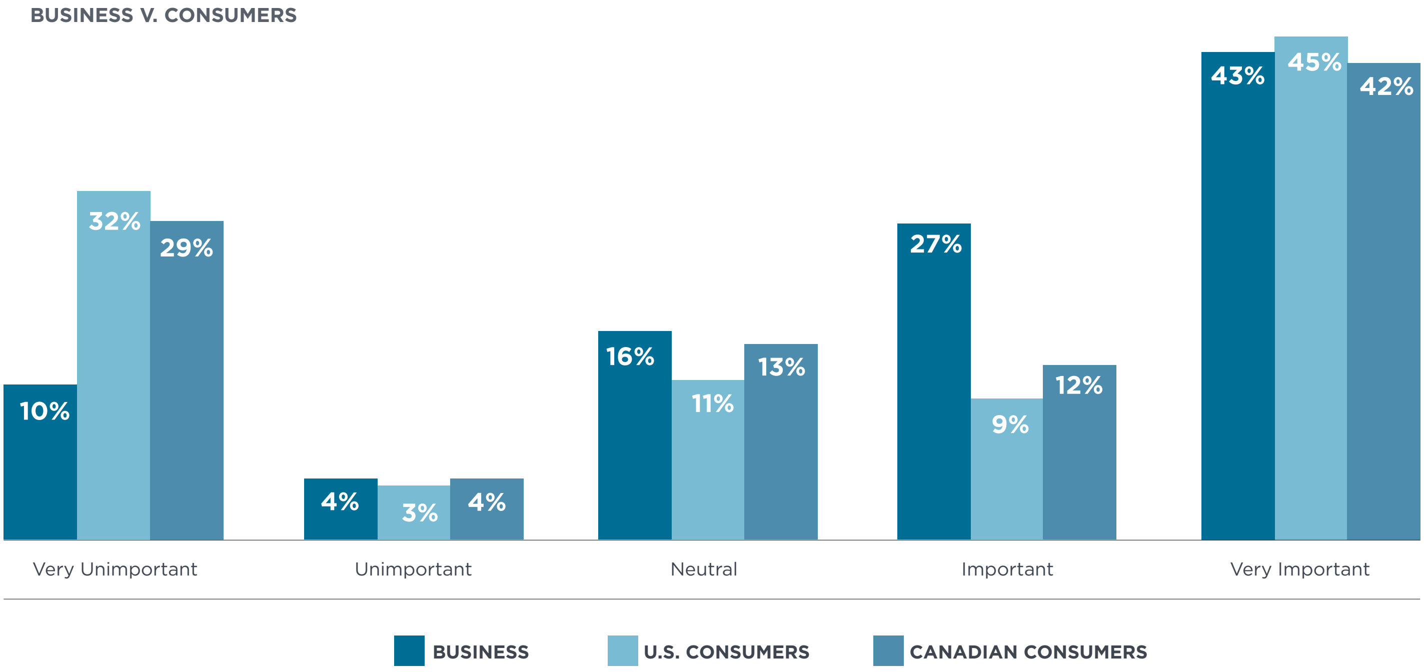


FIGURE 19

**QUESTION: IN THE LAST 12 MONTHS, WHAT DO YOU ESTIMATE YOUR ORGANIZATION'S TOTAL INVESTMENT IN CYBERSECURITY TO BE (IN US $)? THINK OF YOUR EXPENSES WITH VENDORS OF PRODUCTS/SERVICES AND LICENSES, NOT INCLUDING PERSONNEL.**

| | 0-5 EMPLOYEES | 6-10 EMPLOYEES | 11-49 EMPLOYEES | 50-249 EMPLOYEES | 250+ EMPLOYEES |
|---|---|---|---|---|---|
| MEDIAN INVESTMENT PER COMPANY | $200 | $500 | $4,250 | $10,000 | $65,000 |

As expected, annual investments in cybersecurity vary with the size of the company, as highlighted in Figure 19 above.

Since the threat of cybersecurity is real, and action is important, a fundamental question organizations must answer is: How much should they invest in cybersecurity? Gordon and Loeb developed a model based on cost-benefit analysis to help answer this question.[18] Their framework provides a useful guide for organizations trying to find the right level of cybersecurity investment. A simplified and adapted version of their model can be summarized in the five steps on the following page.

[18] http://www.scirp.org/journal/PaperInformation.aspx?paperID=64892

STEP **1** **ESTIMATE LOSS**

For each information set in your organization, estimate the potential loss that you could incur in a cybersecurity breach **($LOSS)**.

For example all your organization's emails, your customer database and your employee list.

STEP **2** **ESTIMATE RISK**

For each information set in step 1, estimate the probability of loss from a cyber breach of that data **(%RISK)**.

STEP **3** **IDENTIFY INVESTMENTS**

For each information set in step 1, identify the potential investments that you could make in cybersecurity **($INVEST)**.

STEP **4** **ESTIMATE SAVINGS**

For each potential investment in step 3, estimate the reduction in the probability of a cyber breach due to the additional cybersecurity investment **(%SAVE)**.

STEP **5** **CALCULATE**

Compare the investment cost **($INVEST)** to the potential savings where: **Potential Savings = ($LOSS) X (%RISK) X (%SAVE).**

**As long as the potential savings exceeds the cost of investment, then it is a cost-effective measure that should be implemented.**

The explanation of the model described above, demonstrates the probability of loss of money due to cyberattacks and can be used by businesses to help them assess their risk and reflect on their cybersecurity effectiveness. For example, let's assume a company has determined that the current probability of losing up to $1,000,000 in the next 12 months ($LOSS) is 4% (%RISK) from a cyber breach. If said business could reduce its risk by 50% (%SAVE), the potential savings would be $20,000 ($1,000,000 X 4% X 50%). Therefore, as long as the investment cost ($INVEST) for the 50% (%SAVE) is less than the potential savings of $20,000, then the investment would be worthwhile. According to Gordon and Loeb, the maximum a company should invest in cybersecurity is approximately one-third of the potential cybersecurity loss (i.e., 37% X $LOSS X %RISK) that it could incur.

It is important to note, though, that determining the Return on Cybersecurity Investment (ROCI) can best be described as a puzzle, due to ongoing changes and challenges in the digital threat landscape and the fact that no matter how protected a company may be, hackers can eventually find a way in. That is why cybersecurity efforts should focus on risk management instead of risk mitigation.[19]

[19] https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity

# BUILDING A BETTER FUTURE

Cybercrime continues to grow rapidly around the world, with annual costs to the global economy estimated to reach over US$2 trillion by 2019.[20] Yet, there is still much that can be done to educate, support, and empower smaller businesses to be cyber secure, to dispel misconceptions, and to help make cybersecurity a priority for smaller organizations.

Spending millions on security technology can certainly make an executive feel safer, but investing wisely and effectively is paramount, primarily for smaller businesses that do not have the same resources as larger organizations. The dynamic nature of the cybersecurity environment – threats escalating rapidly, new technologies introduced constantly, and operational practices evolving quickly – makes it dangerous for cybersecurity executives to rely solely on experience and instinct in making decisions.[21] Although measuring cybersecurity performance is hard, it is necessary that we move in that direction.

In a world increasingly digital and with ever more sophisticated cybercriminals, cybersecurity continues to be a pressing concern for everyone and should become an increasingly critical management issue. Businesses should continually aim to become high reliability organizations (HRO) which operate under very challenging conditions and have succeeded in minimizing the risk of accidents.[22,23] These organizations: a) are sensitive to operations (i.e., each employee pays close attention to operations and maintains awareness as to what is or isn't working); b) are reluctant to accept "simple" explanations for problems; c) defer to expertise and listen to people who have expert knowledge of the task at hand; and d) are prepared in how to respond to failures, and to continually find new solutions.

We hope this report will aid in the continuous support of our community of trusted businesses and the marketplace at large by helping increase awareness about this complex issue among smaller businesses; by helping clarify the real risks associated with cyberattacks and the potential financial and reputational losses; by sharing experiences from other businesses in their efforts to be cyber secure; and by informing key influencers about the obstacles hindering the advancement of cybersecurity efforts among this important market segment.

We recommend an increase in cybersecurity programs focused on smaller businesses, which will encourage further education and awareness efforts. Another area of focus should be public education on cybersecurity frameworks and cybersecurity effectiveness and cost effectiveness. By using the statistics and recommendations laid out in this report, many smaller businesses can begin putting effective plans and activities in place before a breach occurs.

[20] https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5cf192c33a91
[21] http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-blog/the-pitfalls-in-measuring-cybersecurity-performance
[22] https://hbr.org/2003/04/sense-and-reliability
[23] https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

# AUTHORS/CONTRIBUTORS

**BILL FANELLI** is chief security officer for the Council of Better Business Bureaus (CBBB), the umbrella organization for BBBs across North America. Mr. Fanelli initially worked with CBBB as interim chief information officer during a major phishing scam in 2012, and permanently returned as CSO in 2014. Mr. Fanelli has a wide breadth of information security experience, including over 25 years of assessing Critical Infrastructure Protection (CIP) IT and SCADA (Supervisory Control and Data Acquisition) systems, as well as administering NIST 800-53 Controls on Federal Information Security Management Act (FISMA) systems. For the last 11 years, his focus has been in the deployment of data-center, desktop and network security solutions in enterprises with 300,000+ devices. Mr. Fanelli is also primary author of the BBB *5 Steps to Better Business Cybersecurity Training.*

**DR. RUBENS PESSANHA**, PMP, SPHR, GPHR, senior director of market research, insights and strategy, with CBBB, has more than 25 years of global experience in marketing, strategic organizational development, project management and market research. He has presented at conferences in the U.S., Japan, South Africa, Belgium and his native Brazil. A production engineer with an MBA, he completed his doctorate at George Washington University this summer.

**AMY GWIAZDOWSKI** is the director of internal strategic communications for CBBB, actively engaging with BBBs across North America to better understand their needs. Before joining CBBB, she was the communications director for a business trade association for companies with employee stock ownership plans (ESOPs) in Washington, DC. Previously, she spent a few years working for the publishing industry's trade association, where she focused on First Amendment and copyright issues.

**ALEXIS CHNG-CASTOR**, director of brand creative at the Council of Better Business Bureaus, is an experienced marketer and creative director with an award-winning brand portfolio. Native to Singapore and fluent in three languages, she leverages her knowledge and experience with the Asian markets in all aspects of marketing and design. During her free time, she channels her love for design into her personal projects.

**GERALD AUGER,** a senior information security analyst at the Medical University of South Carolina and managing partner at Coastal Information Security Group, has 12 years of information security industry experience with a focus on assessing and managing risk, compliance, governance and program management. Mr. Auger holds a Master's of Science (MS) in Computer Science, an MS in Information Assurance, and is a doctoral candidate in cybersecurity at Dakota State University. Mr. Auger's dissertation research investigates the effectiveness of the NIST Cybersecurity Framework (CSF) on small and medium-sized businesses (SMB).

We also want to express our sincere thanks to: a) the Internet Security Alliance for their work on advancing cybersecurity and for letting us use their study on cybersecurity controls; b) Lawrence Gordon, Ph.D. and Martin Loeb, Ph.D., both professors from the University of Maryland's Robert H. Smith School of Business, for their seminal work in the field of cybersecurity effectiveness and their kindness to let us use some of it in this report; b) Scott J. Shackelford, J.D., Ph.D., Cybersecurity Program Chair, Indiana University, and Anne E. Boustead, J.D., Ph.D., now an Assistant Professor at University of Arizona, who participated while a Postdoctoral Fellow at Harvard Kennedy School, for their feedback and generosity to let us borrow one of their questions to use in our study.

# THANKS TO THE FOLLOWING BBBS THAT MADE THIS PROJECT POSSIBLE

BBB of Upstate New York

BBB of Metropolitan New York

BBB of Chicago & Northern Illinois

BBB of Central Ohio

BBB of Los Angeles & Silicon Valley

BBB of Saskatchewan

BBB Serving Nebraska, South Dakota, Kansas Plains & SW Iowa

BBB of Hawaii

BBB of Eastern North Carolina

BBB Serving North Alabama

BBB Serving Northern Colorado and Wyoming

BBB of Mainland British Columbia

BBB Serving Connecticut

BBB Serving Wisconsin

BBB Serving Arkansas

BBB of Greater Maryland

BBB Serving Central and Western MA and Northeastern Connecticut

BBB of Southern Colorado

BBB of Mexico

BBB is deeply committed to building and advancing a better marketplace, a trusted marketplace for all. From small community stores to multinational enterprises, BBB has been on the forefront of positive marketplace change by partnering with leading companies committed to the best practices of business ethics, marketplace excellence, and effective industry self-regulation. Trust always matters.

BBB®

Council of Better Business Bureaus
3033 Wilson Blvd., Suite 600
Arlington, Virginia 22201 USA
703-276-0100
**www.bbb.org**
**5Steps@council.bbb.org**