CYBERSECURITY

FOR SMALL BUSINESSES

Introduction

You've probably read about or heard of a cyberattack within the past month. Cyberattacks are on the rise and cybersecurity incidents and data breeches are regularly making headlines. In today's cyber threat landscape, all businesses, large and small are at risk for an attack. Cyber threats are a serious risk factor for all businesses.

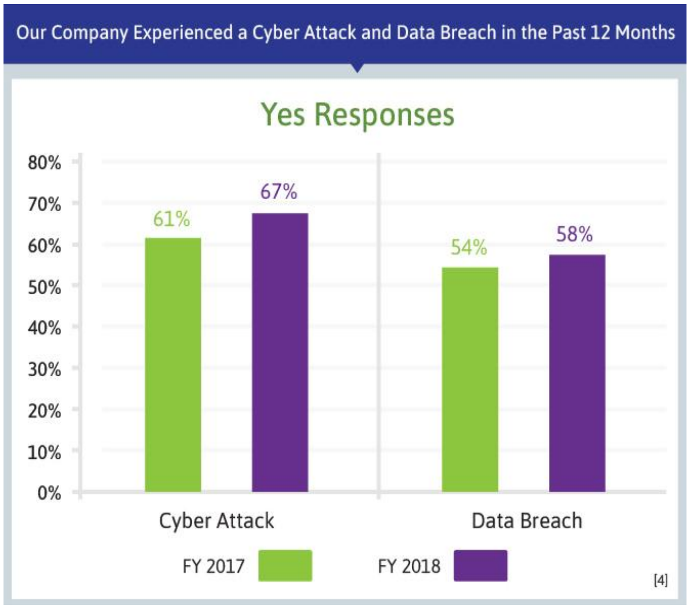
You may think your business is too small for a cybercriminal to bother with but, to cybercriminals, a small business is an easy and valuable target. Cybercriminals are no longer limiting their attacks to large multinational corporations. Many are increasingly targeting small and medium-sized businesses (SMBs). In fact, small businesses often face greater risks since they tend to lack the advanced security protections of large companies. This leaves them vulnerable, making them easy prey for an attacker.

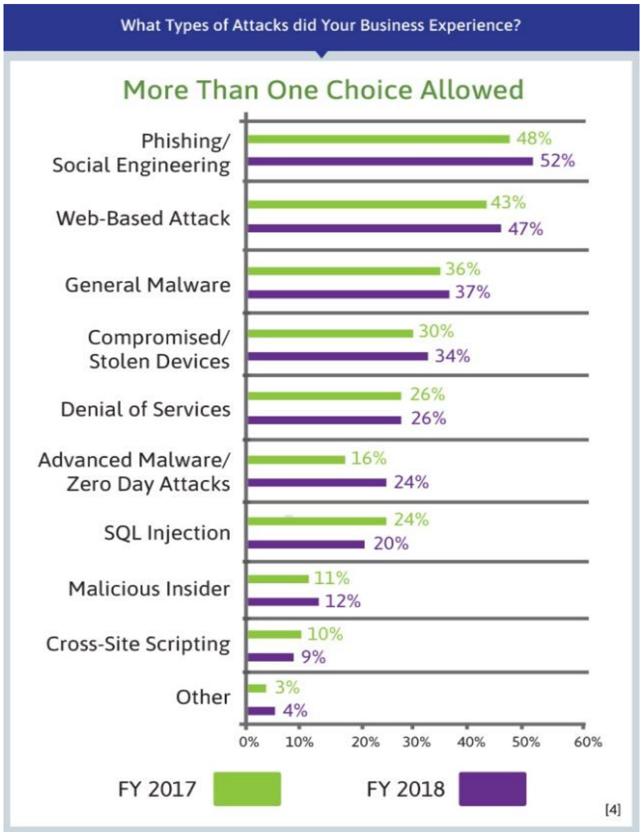
The stakes are high; the impact of a cyberattack on a small business can be devastating. Even a minor incident that results in a few hours of downtime or the inability to access critical data can temporarily cripple a small business and may even shut the doors permanently. The fallout from an attack can result in the loss of revenue, customers, and may result in fines and irreparable damage to the brand, making it difficult to attract new customers, partners, and suppliers.

Small business leaders need to educate themselves and become proactive by becoming familiar with the most common threats and learn the tools and techniques to make their business more resilient. Many small businesses do not have the resources and expertise of large businesses although - *money and talent does help*. You don't need a million-dollar budget or a team of cybersecurity PhDs to get started. There are simple and cost-effective steps that can be taken to get started — regardless of the size of your company or your technical ability. Understanding and following the recommendations outlined in this guide will help.

The Risk to Small Businesses

In 2018 we saw an increase in Cyberattacks on SMBs. [4]

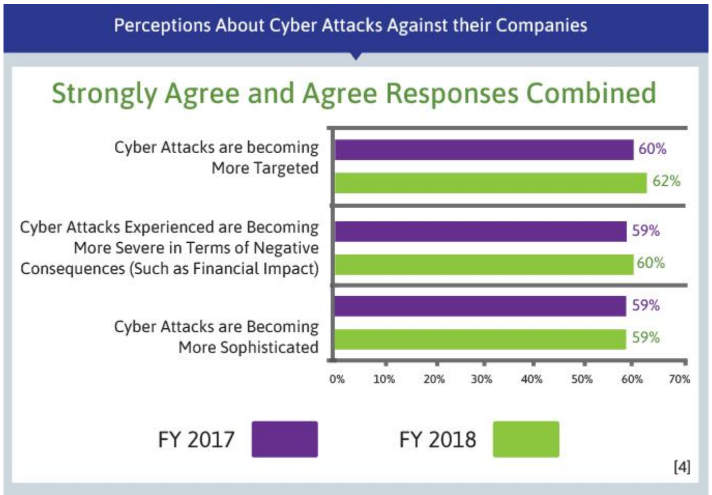




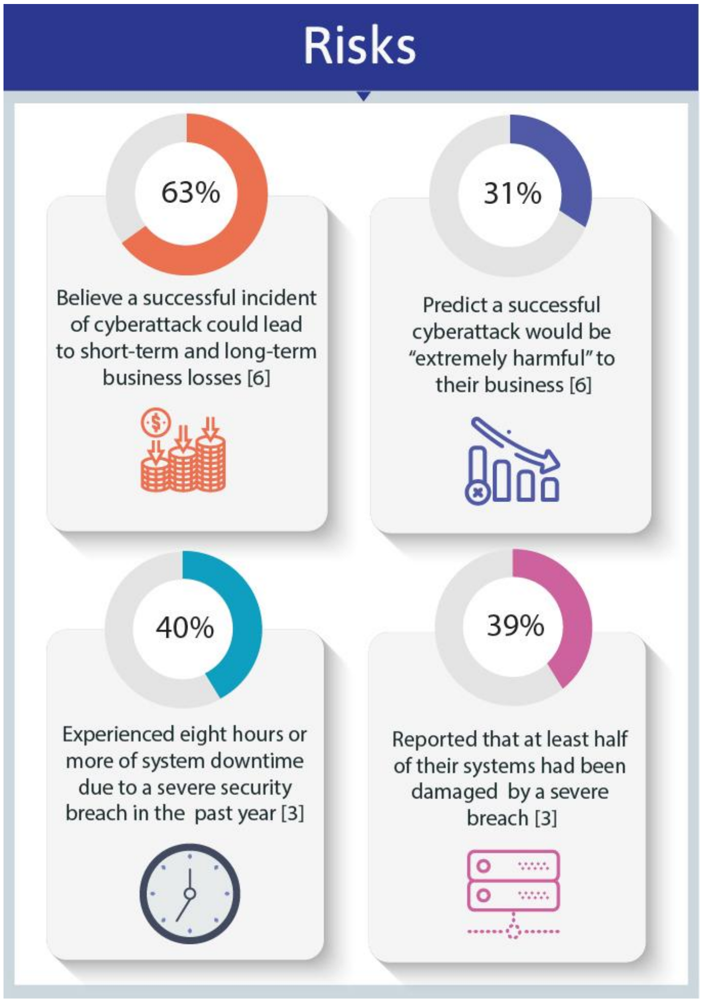
Increasingly, small and mid-market businesses are the focus of attacks [1] and often serve as a launch pad or conduit for larger campaigns.[3] Perhaps the most pervasive reason is that many small businesses simply don't believe a cybercriminal or hacker is interested in stealing anything they have. When confronted with the possibility of a cyberattack, many small business leaders believe they are too small to be of any interest to a cybercriminal or hacker. Others simply accept the risk and take a *"We'll deal with it if it happens"* approach, claiming they have neither the financial means nor technical expertise to mount a reasonable defense. There are also those who believe cybersecurity is an IT issue and assume their technology service provider, cloud service provider or third-party software provider is taking care of cybersecurity for them. Many providers follow a "shared responsibility" model which requires the customer to assume and manage some security functions.

Cybercriminals and hackers have taken notice, and many have shifted their focus and are now targeting SMBs because they know these businesses are not as well defended. SMBs now face many of the same cybersecurity risks as larger companies.

A recent report by the Ponemon Institute reported that small business leaders say cyberattacks against their companies are targeted, sophisticated, and severe. [4]



The resulting damage of an attack and the cleanup effort that is required in the aftermath can cost a business hundreds of thousands of dollars and more in some cases. The Better Business Bureau polled small business leaders and asked: "*How long could your business remain profitable if you permanently lost access to essential data*?" More than 50% reported that they would be unprofitable in less than one month. Only 35% said they could remain profitable for more than three months. [2]

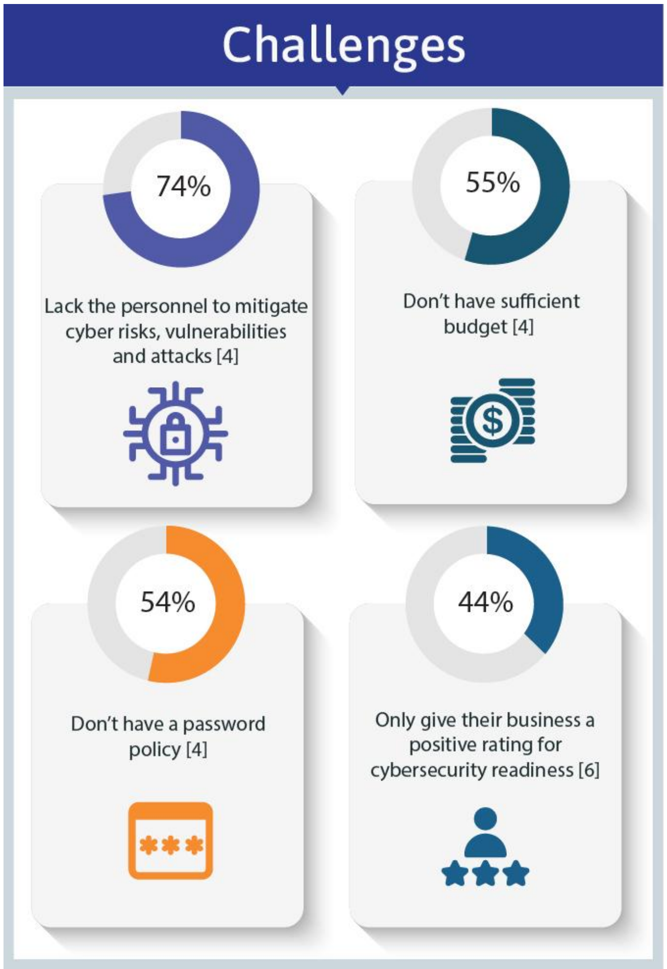


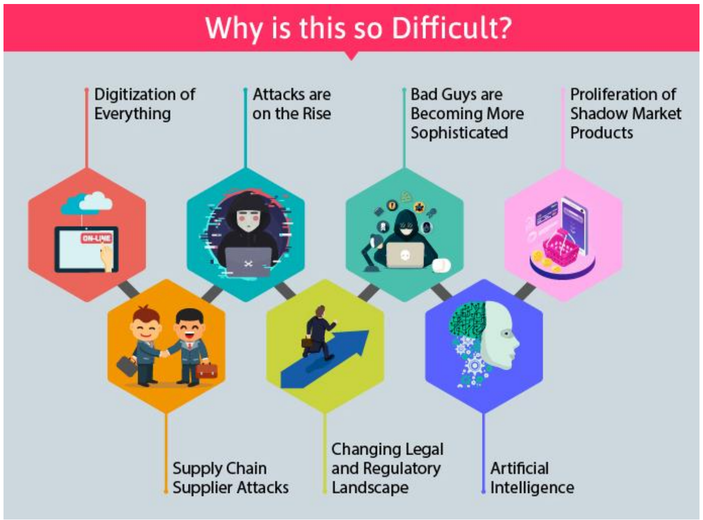
The increasing threat and potential impact of a cyberattack has forced small business leaders to place Cybersecurity into the "Business Critical" category. Business leaders must devote time, resources and make a serious commitment to cybersecurity or risk the very survival of their business. 20% of all SMBs predict there is a high-to-definite likelihood their business would not survive at all after a successful cyberattack. [6]

The Challenges

It is becoming increasing difficult for small businesses to keep pace with the advances in technology. Technology is an enabler, giving small businesses the ability to operate faster and more efficiently than ever before. They now have the ability to engage with and service customers around the globe. Doing business in this fast paced and complex environment places additional pressure on small business leaders to not only learn how to navigate this new landscape but also how to protect themselves in this ever-changing environment.

Many small business leaders report they are struggling to keep up.




Why is this so Difficult?
Digitization of Everything
Attacks are on the Rise
Bad Guys are Becoming More Sophisticated
Proliferation of Shadow Market Products
ON-LINE
Supply Chain Supplier Attacks
Changing Legal and Regulatory Landscape
Artificial Intelligence

Threats

Many small business leaders don't believe a cybercriminal would launch an attack against their business because they are too small. The thing to remember is that Cybercrime is just that, crime. Those who are looking to steal and destroy in the physical world are extending their reach into the digital domain. For many of them it's nothing personal, it's just business. Since many small businesses are collecting sensitive and confidential data, SMBs have become a tempting and easy target for cybercriminals and hackers.

The cast of potential "Bad Guys" who want to harm your business is long and varied. They range from highly sophisticated and well-organized criminal organizations, many of which operate with impunity across the globe, to the disgruntled insider and many others in-between.

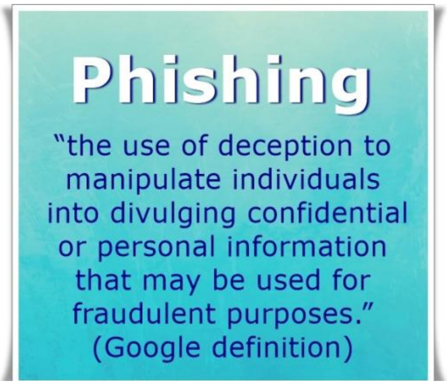
Threats

The “Bad Guys”

- **Cybercriminals** - motivated by profit, these individuals are involved in fraudulent financial transactions, identify theft.
- **State Sponsored** – Nation States who target other governments and private entities to steal intelligence, IP, or to conduct destructive activities.
- **Cyberterrorists** - use violence to achieve their goals, they target critical infrastructures and govt agencies
- **Cyberwarriors** - are nationally motivated citizens who may act on behalf of a political party or against another political party that threatens them.
- **Corporations** - breach security boundaries and perform malicious acts to gain a competitive advantage over their competitors.
- **Script kiddies** - typically individuals who are learning to hack.
- **Hacktivists** - driven by ideology and political motives. They focus on maximizing disruption and causing embarrassment to their targeted victims.
- **Insiders** - disgruntled employees, former employees, suppliers and partners who know how your business runs and have access to systems and data. *Potentially the most dangerous of all.*
- **Online Social Hackers** - are skilled in social engineering, these attackers are frequently involved in cyberbullying and identity theft.

Common Threats

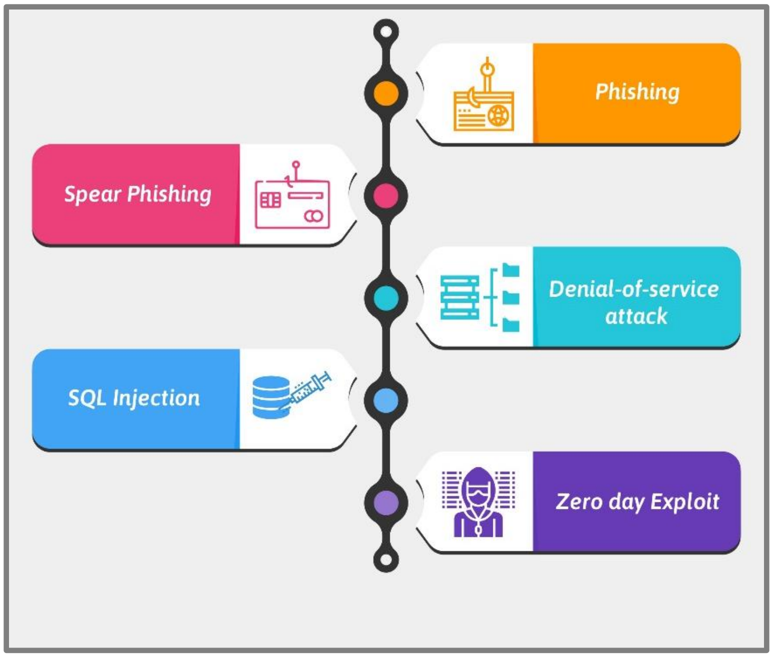
Now that you know who the attackers are, let’s take a look at some of the most common types of attack. Social engineering continues to be the number one attack technique used against SMBs.[4] Cybercriminals are using Social engineering techniques to trick employees into installing malicious software (malware). These attacks typically come in the form of an email from what appears to be a trusted source. When the receiver opens the attachment or clicks on a link in the email, malicious software is installed on the device.



Phishing

“the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.” (Google definition)

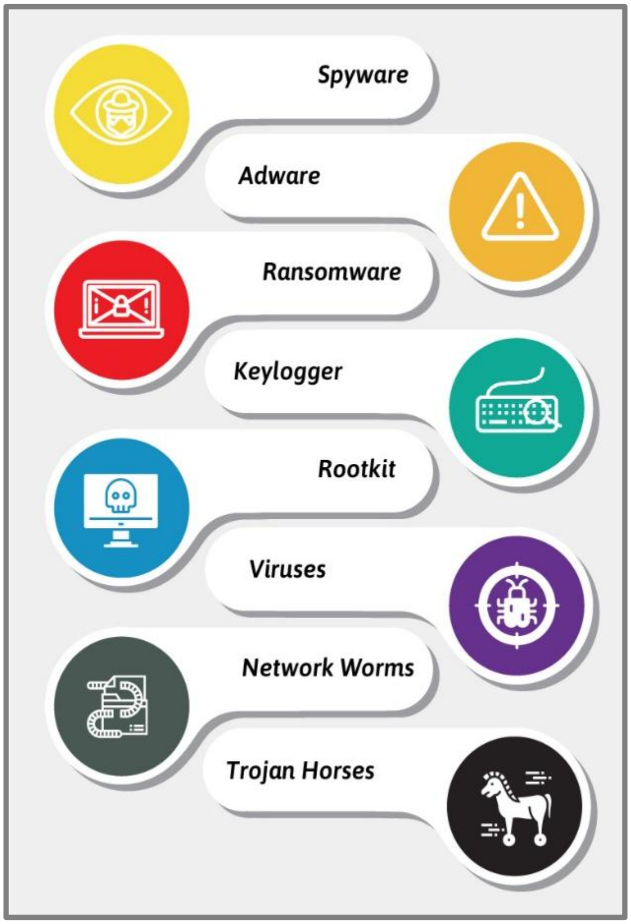
Common Attacks

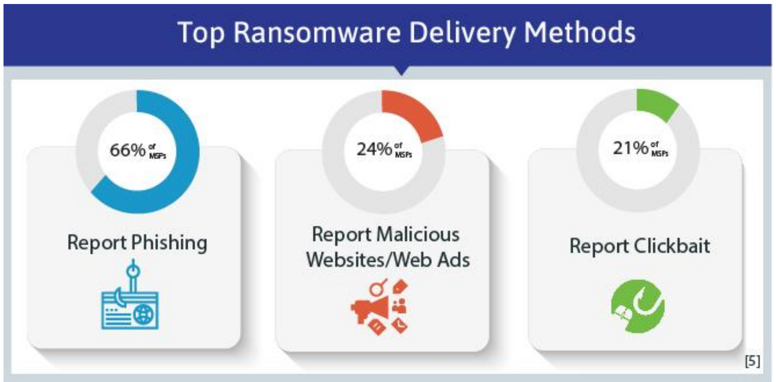


- **Phishing** sends fraudulent communications that appears to come from a trusted source usually in the form of an email.
- **Spear Phishing** is a targeted type of phishing.
- **DoS** - The denial-of-service attack floods servers, systems, or networks with traffic to overload system resources.
- **SQL Injection** - An attacker inserts malicious code (*malware*) into a server and forces the server to reveal information.
- **Zero-day exploit** – Attackers take advantage of a recently announced vulnerability before a patch or solution is available.

Types of Malware

- **Spyware -** gathers information without the user's knowledge
- **Adware** - presets ads that are generally unwanted
- **Ransomware -** locks or encrypts data
- **Keylogger -** secretly records keystrokes and screens
- **Rootkit** - used to hide other malware by modifying the Operating System
- **Computer Viruses -** designed to alter the way a computer operates and spread to other computers.
- **Network Worms -** a piece of self-replicating code designed to spread itself across computer networks.
- **Trojan Horses -** gains access to a system by hiding within an apparently legitimate application.



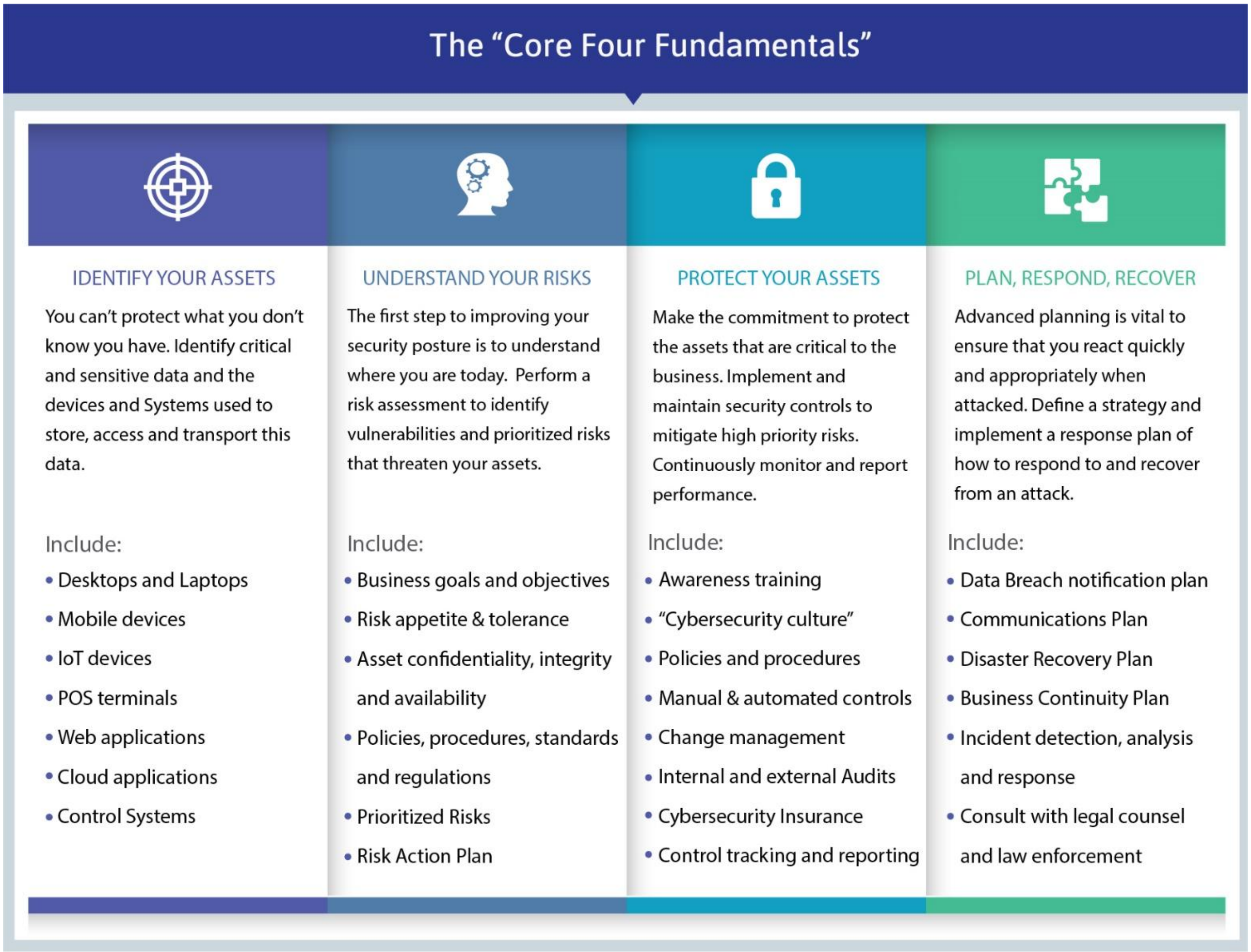


[5]

One of the most dangerous types of malware is ransomware that threatens to encrypt and/or erase data unless a ransom is paid. 2018 saw a rise in ransomware attacks against small businesses. A survey of 2,400 managed services providers (MSPs) reported that 79% of those MSPs reported ransomware attacks against their SMB clients. 92% of those MSPs predict the number of ransomware attacks will continue at current, or worse, rates. [5]

Protecting Your Business

The threat landscape changes daily but, that should not stop you from following some basic steps to start improving your cyber-defenses. Regardless of the size of your business there are some fundamentals to keep in mind as you begin to create your Cybersecurity strategy and plan. Below are what we call the **Core Four Fundamentals** that provide a basic strategy to start organizing your cyber-defenses.



The "Core Four Fundamentals"

IDENTIFY YOUR ASSETS

You can't protect what you don't know you have. Identify critical and sensitive data and the devices and Systems used to store, access and transport this data.

Include:

- Desktops and Laptops
- Mobile devices
- IoT devices
- POS terminals
- Web applications
- Cloud applications
- Control Systems

UNDERSTAND YOUR RISKS

The first step to improving your security posture is to understand where you are today. Perform a risk assessment to identify vulnerabilities and prioritized risks that threaten your assets.

Include:

- Business goals and objectives
- Risk appetite & tolerance
- Asset confidentiality, integrity and availability
- Policies, procedures, standards and regulations
- Prioritized Risks
- Risk Action Plan

PROTECT YOUR ASSETS

Make the commitment to protect the assets that are critical to the business. Implement and maintain security controls to mitigate high priority risks. Continuously monitor and report performance.

Include:

- Awareness training
- "Cybersecurity culture"
- Policies and procedures
- Manual & automated controls
- Change management
- Internal and external Audits
- Cybersecurity Insurance
- Control tracking and reporting

PLAN, RESPOND, RECOVER

Advanced planning is vital to ensure that you react quickly and appropriately when attacked. Define a strategy and implement a response plan of how to respond to and recover from an attack.

Include:

- Data Breach notification plan
- Communications Plan
- Disaster Recovery Plan
- Business Continuity Plan
- Incident detection, analysis and response
- Consult with legal counsel and law enforcement

How Much Will It Cost?

This is typically the first question many small business leaders ask when discussing Cybersecurity and it is a difficult one to answer without having in-depth knowledge of the business. Ultimately, it comes down to the business to determine what is an adequate level of security. Reducing cybersecurity risk to an acceptable level is dependent on the value of the asset at risk, the worst-case scenario if the asset was stolen, destroyed, or compromised and of course, what the business can afford to spend on security. For example, if you own a small business and someone steals your supplier list, the attack would probably not cripple your business or shut your doors. But if you own an online eCommerce business, and a cybercriminal steals your unencrypted customer database that contains customer name, payment card information, email address, home address and phone number, the consequences could be devastating to your business. Exactly how devastating? Estimates vary. Some cybersecurity experts report the average cost of a data breach for a small business in North America at over $100,000 dollars. More than 54% of all cyberattacks result in financial damages of more the $500,000. [3] That amount of money is enough to put many SMB's out of business – permanently. If you have customers in the European Union, that number can increase ten times.

The fines that can be levied under the EU General Data Protection Regulation (GDPR) [7] are potentially huge. Businesses face fines of up to 4% of their annual turnover or €20 million for an actual breach of someone's personal data, whichever is higher. The "*whichever is higher*" is the key phrase.

Consider these questions when determining how much to invest in cybersecurity for your business:

1. What is the risk appetite and tolerance of the business? How much risk is the business willing to accept and capable of absorbing without severely affecting operations.

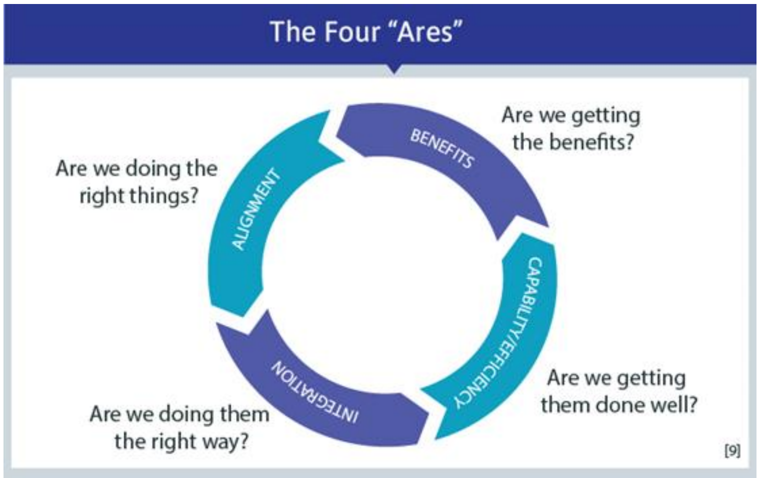
2. What are the critical assets to protect? Remember, assets can be tangible and intangible. They include data, hardware, software, people, processes, intellectual property, brand reputation, professional relationships, etc.

3. What is the value of the asset? Consider the replacement cost *AND* the cost to the business if the confidentiality, integrity or availability of the asset was compromised.

4. Would the business survive if the asset was stolen or permanently unavailable? What would be the impact on your business? Would you be able to continue?

Getting Started

Some key questions to answer as you get started.


The Four "Ares"
Are we getting the benefits?
BENEFITS
Are we doing the right things?
ALIGNMENT
CAPABILITY/EFFICIENCY
Are we getting them done well?
INTEGRATION
Are we doing them the right way?
[9]

The most critical area to focus on (not to mention most influential) are your employees. Employees can become your greatest ally or the greatest threat.

When educating and training your employees, strive to establish a "cybersecurity culture" that enables a virtuous circle in which employees, understanding their roles and responsibilities act as human firewalls to enable the enterprise to respond, either by preventing the attack or speeding up the detection, response and recovery cycle. [8]

Cybersecurity is complicated. To strengthen your defenses, you need the right balance of technology, process, skilled resources and time, things that are in short supply in many small businesses. You need an experienced partner such as PamTen, who can help you develop a strategy and a plan that meets the needs of your business.

Visit us to learn more or give us a call to understand how we can help protect your business.

John Mendes, CRISC, PMP
VP Solutions

Don Philmlee, CISSP, PMP
Security Consultant

Resources

1. https://www.nist.gov/itl/smallbusinesscyber - National Institute of Standards and Technology (NIST) The small business cybersecurity corner provides free information produced by federal agencies, including NIST and several primary contributors, as well non-profit organizations and several for-profit companies
2. https://www.sba.gov/course/cybersecurity-small-businesses/ - Half hour basic introduction to cybersecurity presented online by Small Business Association.
3. https://www.dhs.gov/publication/stopthinkconnect-small-business-resources - Federal Department of Homeland Security (DHS) guides and links to resources for small business including best practices and technical guidance
4. https://www.fcc.gov/cyberplanner - Federal Commerce Commission tool to help a small business create a security plan
5. https://www.us-cert.gov/ccubedvp/smb - US Computer Emergency Readiness Team (US CERT) resources to help small business create or improve a cybersecurity program.
6. https://staysafeonline.org/cybersecure-business/ - National Cyber Security Alliance program helping small and medium-sized businesses (SMBs) learn to be safer and more secure online.
7. https://www.ftc.gov/tips-advice/business-center/small-businesses - Federal Trade Commission guide and resources for protecting small businesses.
8. https://www.nsa.gov/what-we-do/cybersecurity/#professional-resources - National Security Agency (NSA) technical how-to guides and information sheets for destroying media or security networks and computers.
9. https://www.ic3.gov/preventiontips.aspx - Internet Crime Complaint Center; includes form for reporting and how-to guides to guard against being a victim.
10. https://www.sans.org/security-awareness-training/resources - SANS free security awareness posters, videos, and resources.
11. https://www.fbi.gov/investigate/cyber - FBI overview for areas of cybercrime with resources for training of all ages in best practices.
12. https://www.infragard.org – FBI's service organization for partnership between private sector and FBI in promoting awareness and best practices against cybercrime. Open to businesses and individuals.
13. https://www.cisecurity.org/resources/newsletter/ - Center for Internet Security cyber newsletters. Oriented toward the not-necessarily-technical reader for news, threat awareness, and best practices.

Sources

1 "Cyberthreats and Solutions for Small and Midsized Businesses", Vistage Research Center, 2018.
2 "2017 State of Cybersecurity Among Small Businesses in North America", Better Business Bureau, 2017.
3 "Cisco 2018 Annual Cybersecurity Report", Cisco 2018.
4 "2018 State of Cybersecurity in Small & Medium Businesses," Ponemon Institute LLC, 2018.
5 "Datto's State of the Channel, Ransomware Report", Datto, 2018.
6 "AppRiver, Cyberthreat Index for Business: Q1 2019", AppRiver, 2019.
7 GDPR EU.org
8 "Narrowing The Culture Gap For Better Business Results", ISACA/CMMI Institute, 2018.
9 "The Information Paradox—Realizing the Business Benefits of Information Technology", 2007, Fujitsu Consulting (Canada) Inc.