AMERICA'S SBDC FLORIDA

The Florida SBDC Network Byte-Size Program:

Cybersecurity Basics for Small Business

→ FloridaSBDC.org/Cybersecurity

Helping Businesses Grow & Succeed

Contents

NOTE: These materials are intended to provide information to assist small businesses consider key cybersecurity concepts, to share ideas for reducing cyber risk, and to identify helpful resources from multiple public and private organizations. However, no single technology or program can eliminate all cyber risk nor can they guarantee protection from constantly evolving digital attacks. It is always best to consult IT security and legal professionals to understand your responsibilities and to manage the specific cyber risks associated with your business.

Introduction

Over the last two decades, the rise of the Internet and proliferation of digital technologies have changed the way that Florida small and family-owned companies do business. Technology has been an enabler, making operations more efficient, speeding and improving customer service, and supporting expansion into new markets around the globe. In fact, small and medium-size Florida businesses drive over 66% of the state's $153 billion export value alone! These are the clear economic benefits.

But there is a dark side.

Small businesses are, for a variety of reasons, extremely vulnerable to malicious cyber attacks. Perhaps the most critical (and pervasive) reason is that many small business owners just don't always understand the risk. In fact, an astonishing 87% of small business owners do not regard their own business as being at risk of cyber attack, despite the fact that half of all small businesses in the United States were hacked over the past 12 months.[1] Many small business owners believe they are immune from malicious interest simply because they can't imagine they have data worth stealing. Others can't imagine that they could possibly muster the resources to mount a reasonable defense even if they admit the risk. The dangerous and ill-advised cry: "It would never happen to us!" is heard up and down Main Street.

Whether they are relying on good luck and hoping for the best, or whether they are simply overwhelmed by what they perceive as a costly big business sort of problem, small business owners are in a precarious position regarding cybersecurity. Hackers are now targeting small businesses precisely because they are known to have fewer resources for digital defense and can appear to hackers to be easy prey. Ignoring the risk, however, or postponing preventive measures, can open a small business up to significant liabilities and can put its very existence in jeopardy.

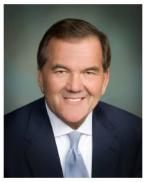
The good news is that there is hope. The Florida SBDC Network has created the ***Byte-Size Small Business Cybersecurity Program***. This easy-to-digest guidebook and toolkit of affiliated resources provide user-friendly information that can help make your company more cyber-secure in an increasingly perilous 21st Century environment.

While no technology or program can stop every attack, taking basic precautions can reduce your technical risk and make your company a less attractive target. Moreover, it can save an enormous amount of headache and, potentially, your business.

More importantly, the Florida SBDC Network Byte-Size program means that you are not alone. For more than 40 years, Florida SBDC Network consultants have helped small businesses overcome challenges to their growth. Today, the Florida SBDC Network is partnering with the US Chamber of Commerce, federal, state and local agencies and other organizations to build these practical resources to help you meet the challenges of doing business in cyberspace. Together, we will work with you to not only better understand threats, but also to leverage enhanced cyber readiness as a mark of reliability and competitive advantage for Florida's small businesses.

Michael C. Myhre

Michael W. Myhre
CEO and Network State Director
Florida SBDC Network



Tom Ridge

The Honorable Tom Ridge
First Secretary of Homeland Security
Chairman, US Chamber of Commerce
National Security Task Force

[1] Ponemon-Keeper *2016 State of SMB Cybersecurity* report

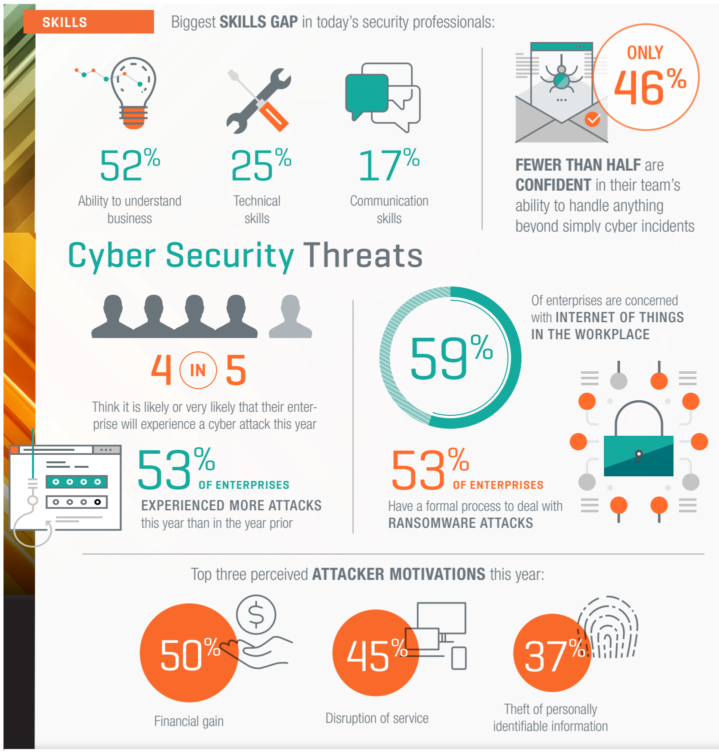
Section 1: **Basic cybersecurity threats to small businesses**

Let us first consider the very real threats that are likely to directly impact small businesses. We shall look both at the types of people that would seek to do harm, and also at the typical tools they will likely use to do harm.

The bad guys

The reasonable question that many small business owners ask when confronted with the possibility of a cyber attack is: Who would want to do me harm? The simple fact is that many cybersecurity threats originate with evil people motivated by evil intentions. These villains are actively seeking to cause mischief, to steal and destroy in the digital domain just as they do in the physical world—and for a wide array of reasons. For some of them it is nothing personal. It may just be about money, or control, or even just a few laughs. For others it could be highly personal.

The list of people who may seek to do a business harm is long and varied. It could include an unprincipled competitor seeking an advantage by ruining a reputation or disrupting services or stealing customers. While perhaps less pleasant for a business owner to contemplate, it might just be a disgruntled employee or former employee seeking revenge by undermining or destroying their business. It could be thieves intent on breaking in and stealing, though most small business owners tend to believe they are safe from such predators because they are quite sure there are better pickings elsewhere. Do not be deceived. No business is too small to be noticed by bad guys. No small business is immune from attack. Bad guys are in fact especially interested in targeting businesses that do not consider themselves targets precisely because they take few if any precautions at all.



SOURCE: ISACA's State of Cyber Security 2017: Part 2: Current Trends in the Threat Landscape www.isaca.org/state-of-cyber-security-2017

Others who may seek to harm a small business could include curious young hackers doing damage just for the sport or challenge of it. And in the modern world one must consider the unfortunate likelihood that there is involvement by organized crime because hacking can be very big business, or even by state actors, or non-state terrorists whose interests may simply be in destabilization and widespread mayhem. Whether a cyber attack is random and widespread or deliberate and targeted can make a big difference in the overall impact of a security breach. Targeted attacks tend to be more effective and more damaging. Dishonest competitors, disgruntled employees, and thieves are most likely to specifically and deliberately target particular small businesses. Unscrupulous school kids testing their hacking skills, large scale criminal enterprises, state actors, and terrorists are more likely to launch attacks that affect large, anonymous communities of users.

The Insiders

Dangerous insiders could include the kind of disgruntled or former employees with nefarious intent mentioned previously. But an attack on a business from the inside could also come from employees, contractors, or other "trusted" individuals who unwittingly or unknowingly enable attacks or provide hackers with access to systems. In fact, one 2016 survey found that insiders were the cause of "50% of incidents where private or sensitive information was unintentionally exposed."[2] Employees trained to recognize potential threats as well as the establishment of and adherence to clear protocols for network and sensitive data access can help minimize insider risk.

Security vulnerabilities

Adversaries will exploit various types of weaknesses. These vulnerabilities fall broadly into two main categories: Technical and Procedural. It is important to understand the difference because they require different solution sets. Both can have dire consequences for small businesses if they are not adequately addressed.

Technical security vulnerabilities: These include product defects or flaws that can be exploited to breach a system. Technical vulnerabilities are primarily hardware and software issues, and thus fall for the most part under the purview of product vendors such as Microsoft, Adobe, Google, Apple, and so on. While not under his direct control, a small business owner needs to understand how these problems can impact a business.

Procedural security vulnerabilities: These include defects in the processes and policies we use to manage risk. Examples: Failing to establish a business internet and e-mail use policy, neglecting to have employees regularly change security passwords, or maintaining lax security procedures for granting and removing access to key data systems or equipment. These are under the direct influence of the small business owner. It is a responsibility that must not be ignored. We shall discuss this more later.

An exploitable defect in a software program can expected to be patched by the manufacturer. On the other hand, the management of a small business must ensure that these patches are regularly installed on their systems and that people, policies and procedures are in place to get it done.

[2] CERT-Software Engineering Institute-CSO Magazine 2016 U.S. State of Cybercrime report, https://insights.sei.cmu.edu/insider-threat/2017/01/2016-us-state-of-cybercrime-highlights.html

Common threats

Now that we've seen some of the kinds of people who represent a potential threat to small business cybersecurity, let's look at some of the most common tools of their trade. Just being aware of and being able to recognize the tactics typically used, and especially how our own goodness can be used against us, will go a long way toward mitigating much of the external threat.

Malware

Malware is malicious software that is developed with the express purpose of incapacitating or otherwise damaging computers or computer systems. Malware does not come into play by accident. It was written with ill intention. Malware tools can perform whatever bad action its author intends, including (but not limited to) stealing credentials or other information, stealing or extorting money, and sabotaging systems, often by denial of service. Let's take a look at some of the most common types of malware.

> "Last year, cyber criminals launched 430 million new types of malware software out into the world."
>
> SOURCE: How to Protect Your Small Business from Cyber Attacks

Ransomware: Worldwide ransomware attacks have generated a great deal of news. Ransomware is a malware tool that encrypts or "locks up" a victim's files and then displays a message demanding payment in order to recover (decrypt) the data. Ransomware is the attack preference du jour against small businesses because it is a relatively easy type of hacking that provides a fairly reliable and very high return on time investment.[3]

Botnets: The term "botnet" merely describes a network of robots. Botnet malware generally places the victim's computer into a network of other computers, often located randomly throughout the Internet. Each botnet "agent" waits for commands from its controller, often using communications channels like Twitter. The controller can then instruct a vast army of botnet agents to perform some malicious action en masse. More often than not, such botnets are used to overwhelm or flood a victim's network, thus causing a "denial of service" attack.

Denial-of-service (DoS): The purpose of a DoS attack is to deny the victim of its computing or network resources for some period of time, effectively bringing some or all of its business to a halt. The attack is designed to shut legitimate users out of legitimate activities by inundating a system with information such that it cannot be accessed due to overload.

Sabotage: This can include pretty much any deliberate malicious act against a victim's computer or computer system. Files can be deleted. Systems can be erased.

[3] Ransom isn't random: How small businesses can fend off targeted attacks

Applications can be removed. And so on.

Distributed Denial of Service (DDoS): An attacker may take advantage of vulnerabilities to take control of multiple computers (creating a botnet), and then use them all at once to attack another computer or computer system to deny service. It is described as distributed because the attacker uses multiple computers, rather than just one, to launch the denial-of-service attack.[4]

Each of these attacks can be targeted or untargeted. For untargeted attacks, much of the risk can be mitigated by a variety of commonly available remedies such as anti-virus products. That is not necessarily the case for targeted attacks. We'll come back to this in more detail.

Phishing

Phishing is a type of social engineering attack[5] designed to trick the victim into doing something ill-advised on email, such as execute an attachment, click on a link, or unwittingly give away sensitive information. This is generally done by "spoofing" or posing as an otherwise legitimate person, product, or service. Some phishing attacks are extremely sophisticated; bad people are sometimes really good at exploiting human gullibility.

Phishing attacks are among the most prolific problems seen on the Internet today. Some phishing attacks appear to be sent from a trusted service provider such as a bank or credit card company. The phishing message will likely appear to be a genuine communication from the service provider, and will instruct the victim to do something such as "verify your account information for security purposes." It will then direct the victim to an Internet URL (link) where the victim willingly enters their account credentials thinking that they are actually connected to the bank when they are in fact connected to an identical looking malicious system operated by the attackers.

In another type of phishing attack, an email will include a file attachment, that contains malware. When the victim clicks on the file attachment it launches the malware, which will likely run with all of the victim's access and privileges.

Phishing attacks have been widespread on the Internet for roughly two decades, and they show no sign of abating. While some are rather unsophisticated and obviously fake, others are exceedingly difficult to spot, even by trained experts.

Once again, it is critical that we understand the difference between targeted and untargeted attacks. Various security products can detect and block untargeted phishing emails, but blocking targeted attacks is still highly problematic because people are people. As mentioned earlier, social engineering can be highly successful because people often want to please others and generally want to be helpful. Whether it is gullibility or guilelessness is up for debate, but the fact remains that people are often too easily manipulated and are therefore often too easy prey for bad guys.

Among these targeted attacks, Business Email Compromise (BEC) is on the rise.

For example, it can start as an email that arrives in the inbox of a small business bookkeeper. It appears to come from the owner of the business and asks that a wire transfer be made as soon as possible to cover an

[4] See US-CERT: Understanding denial-of-service attacks

[5] Social engineering is "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes." (Google definition)

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
DilbertCartoonist@gmail.com Dilbert.com
WAIT FOR IT
Enter your bank account number.
SCAM.
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.

Adams, Scott. Dilbert. 19 May, 2014.

emergency expense. It all appears legitimate. But it is actually a Business Email Compromise. According to the FBI, this form of cyber scam has increased by an astounding 1300% since 2015.[6] BEC attacks frequently target company finance employees. Having company processes in place to verify significant financial transactions are critical to avoiding be the victim of this method of cyber deception.

Internet of Things (IoT)

The Internet of Things describes the interconnectedness of all sorts of electronic devices through the Internet. It does not so much describe the interconnectedness of the usual and obvious items such as smart phones, smart TVs, and smart tablets that we associate with Internet usage. Instead it describes the less obvious interconnectedness of, for example, automobiles, home security systems, and kitchen appliances that may be less secure, but just as interconnected. These sorts of unsuspected devices are increasingly being targeted for use in such nefarious purposes as eavesdropping and data theft. And they are increasingly being commandeered for use as botnet agents and for DDoS attacks.

> "The Internet of Things arrived in force at this year's International CES, the huge trade show here. But while manufacturers at the event painted a rosy picture of connected grills, coffee makers, refrigerators, and door locks, security experts and regulators warned that the Internet of Things could be a threat to both security and privacy. Hackers have already breached Internet-connected camera systems, smart TVs, and even baby monitors. In one case, someone hacked a networked camera setup and used it to scream obscenities into a baby nursery."
>
> - Molly Wood, The New York Times
> (CES: Security Risks from the Smart Home)
>
> SOURCE: Digital Guardian

[6] Federal Bureau of Investigation: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

IoT devices are playing an ever more important role in today's cybersecurity landscape. Companies are routinely purchasing seemingly dedicated smart devices and connecting them to their internal networks. These devices include security cameras, point of sale terminals, thermostats, and even printers/copiers, and many of them contain security defects that can be and are exploited by attackers. More and more often cyber attacks are showing evidence of malware written specifically to infect popular IoT devices. And this malware is being tailored to perform all manner of malicious actions.

One cannot ignore the question of how the malware gets onto these smart devices in the first place. It can be done via phishing attachments, network access via externally-accessible devices, etc. These initial attacks can be aimed at conventional personal computers (PCs), but once executed, the malware searches the local network for vulnerable IoT devices and infects them if it can. Those IoT infections can rely on unchanged default passwords, hard coded (by the vendor) passwords, or operating system vulnerabilities similar to those found on general purpose computers. Many IoT devices are, after all, built on top of open source operating systems like Linux or common commercial operating systems. Given some level of access, IoT malware can exploit both technical and procedural flaws to gain control of devices. It is therefore vital that IoT device users run their devices securely, and that access to the devices is restricted accordingly.

Application attacks

Today, we all use software applications or "apps" to make the most of technology. For small businesses, examples of apps include programs on your computer for word processing, producing accounting spreadsheets, facilitating online purchases, or web browsing. We also use apps on tablets and smartphones to utilize our favorite social media platforms and to access photos and music.

Apps make so many technology processes more convenient, that you have probably heard the phrase, "there's an app for that!" Unfortunately, cyber criminals apply that phrase in a much different way.

Application software can be maliciously manipulated to steal data from a database server, run attack scripts on other users' PCs, and/or steal user credentials. Business applications, and particularly customer-accessible web applications, are often targets of attacks.

Many small businesses rely on of-the-shelf software to run their Internet presence sales systems. These systems can be extremely vulnerable to both technical and procedural security weaknesses. All application software, just like all desktop computers, should be well maintained and carefully configured with security in mind.

Section 2: **Security matters**

It seems now fairly obvious that small business owners and principals need to pay attention to cybersecurity issues. According to Symantec's *2016 Internet Security Threat Report*, 43 percent of cyber attacks target small business.[7] There is just no getting around the fact that cybersecurity is not a subject that can be safely ignored.

It is true that small business owners have a great deal of responsibility, and have to juggle a lot of important things. But cybersecurity must now fall into the category of "Business Critical". While taking steps may seem like another expense, it should in fact be regarded as an investment in the survival and growth of your business. The price of the alternative is just too high. Sixty percent of small companies go out of business within six months of a cyber attack, according to the U.S. National Cyber Security Alliance, and the Ponemon Institute has calculated that the average cost to a small business for putting things right after a successful attack by cyber criminals is a staggering $690,000, and even higher for mid-size companies.[8]

The time to act is now.

Vulnerabilities become risks

A small business owner might ask why we should care about technical vulnerabilities. After all, aren't the companies that make the software or hardware on the hook if anything goes wrong? Isn't finding and correcting flaws part of their core business responsibility? The answer of course is "Yes," and does it really matter in the end who's to blame if your business collapses?

Technical vulnerabilities, when exploited, can be costly in terms of down time, lost revenue, and the price of containment/repair. There are the after-the-attack costs such as legal expenses that can be stifling for a small business. Moreover, while perhaps somewhat less quantifiably, successful hacks can be equally costly in terms of tarnished reputation and the customer flight that often follows. After all, a good reputation can take years to build up and only moments to destroy. Technical vulnerabilities can impact even the smallest business's bottom line.

7. Small Business Trends: CYBER SECURITY STATISTICS – *Numbers Small Businesses Need to Know*
8. The Denver Post: *60% of small companies that suffer a cyber attack are out of business within six months.*

It's about the customers

Customers want to be confident, even in the smallest business. They expect their online experience with any business, of any size, to be completely secure. And it's a reasonable expectation. Customers should not need to worry that doing business with you could jeopardize the safety of either their property or their very identity. Give them no reason to doubt their choice in your company. Many customers have a natural affinity for small business; they should not be penalized for putting their trust in one. When it comes to reliability and safety, size ought not matter.

Employee considerations

Trusting your employees is one thing—and a very good thing at that. Handing everyone in your company the combination to your private safe is another thing altogether. It's time to understand that the virtual world of IT is just as real and just as subject to violation as your physical office space. In fact, more so. Think through very carefully who needs access to what and why. And then take the steps necessary to prevent unnecessary intrusion.

The same holds true regarding your customers, your vendors, and other third parties. Just because you like them and trust them does not mean you give them the keys to the inner sanctum. Institute very clear and very strong security policies based firmly on the tried and true concept of least privilege.

The *Principle of Least Privilege* is nicely defined thus:

> "Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur. Thus, if a question arises related to misuse of a privilege, the number of programs that must be audited is minimized. Put another way, if a mechanism can provide "firewalls," the principle of least privilege provides a rationale for where to install the firewalls. The military security rule of "need-to-know" is an example of this principle." (Saltzer and Schroeder [Saltzer 75] in "Basic Principles of Information Protection," page 9).[9]

Protecting proprietary information and other private company information is of utmost importance. Consider first how you protect your company's most private information such as payroll and accounting. You need to follow the same precautions with your company's electronic data as you do with any of your company's other secrets. There is actually no difference in terms of importance or scope.

Consider also the different classes of access that you need to allow, and what degree of access is needed by each of the different classes. Employees, for example, will have different access needs than contractors, who will have different needs than customers, and vendors, and so on. You need to

[9] Quoted in US-CERT: Least Privilege

construct an environment that enables business to take place effortlessly and seamlessly, but at the same time doesn't put the business at risk by granting too much access to the wrong people. In other words, use the principle of least privilege; that is, give everyone the least amount of access they need to do their jobs, but no more.

It's a good principle. It's a principle that needs to become the very fiber of your Information Technology security system's being.

Trust considerations

When weighing cybersecurity considerations, small business owners need to find the right balance between trust and security. To some degree that relationship will be driven by your company culture. Information Technology security should mirror the norms of your physical security measures. Consistency is one of the hallmarks of trust, and is crucial to effective security. Employees need security measures and enforcement to be both consistent and predictable in order to both feel trusted and operate comfortably in a secure environment.

It is a basic rule of psychology that people who feel appreciated and trusted are likely to be happier than those who live in a culture of mistrust. So find the proper balance between trust and security that meets your needs and fits with your company's culture. Because a breach can bring a small business to its knees and crush the ability to generate revenue, cyber hygiene and the establishment of effective digital practices are critical to protecting revenues and jobs. When employees understand the important link between cybersecurity and the success of the business, it is easier to establish a team culture that values adherence to company information security policies.

You can find resources for building effective policies and plans in the *Resources and Planning* section.

Regulatory concerns

Small business owners are for the most part free to choose how they protect their company's information. Depending on the sector in which you operate, however, there may be categories of data that require specific protection by law or regulation. And in such cases, the specific treatment required under the law is clearly defined. And it is not optional.

These categories include, among others:

Payment information. Credit card numbers must be protected in compliance with PCI-DSS (Payment Card Industry Data Security Standard), an industry requirement.

Employee privacy data. Certain personally identifiable information (PII), personal health information (PHI), including social security numbers, bank account numbers, and so on must be protected.

Contract information. If your company is a government contractor, you may have specific requirements for protecting the customer's data. Some customers require their data to be encrypted while it's stored. Others require destruction of data at the termination of a contract.

Customer data. Other customer data may also carry with it specific requirements for safeguarding.

The protection and security of these types of data is not optional. It is the responsibility of the small business owner to ensure compliance with all applicable laws, regulations, and contractual obligations.

According to the Better Business Bureau, "At least twenty states have passed laws requiring small businesses to implement procedures to prevent personal information from being disclosed or improperly used. Some states specifically require that small businesses encrypt personal information that is sent over the Internet. Unlike federal laws, these state laws apply to all small businesses — not just those that are financial institutions or health care providers. Additionally, almost every state has passed legislation requiring disclosure of any incidents involving the loss of consumer information."

SOURCE: Digital Guardian

Like it or not, our reliance on technology has changed the way we service customers and manage employees. This means that credit card information, financial records, driver license and social security numbers, and health information previously mentioned are some of the forms of data you may possess and that are addressed by these laws. Understanding responsibilities for the care of customer and other sensitive data and knowing legal requirements should a breach occur are part of doing business in the 21st Century.

In Florida, statutes require that any "sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information" provide notice to the Florida Department of Legal Affairs "of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred."

Further, companies in this situation must send a notification "to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach."[10]

[10] Fla. Stat. §§ 501.171, http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html

Section 3: **Remediation practices**

The importance of remediating cybersecurity vulnerabilities and mitigating cybersecurity threats cannot be overemphasized. There are many tools, tactics, techniques and procedures designed to protect from or respond to cybersecurity threats. Let's take a look at some of the available solutions that are particularly applicable to small businesses, and also get a sense for how these corrective solutions are deployed.

Security fundamentals

First and foremost, we must consider the security objectives (the desired outcomes) and the controls that can be implemented to achieve them.

The list of desired outcomes will certainly include confidentiality, integrity, and availability. It will also include accountability, non-repudiation, and reliability. Each of these objectives has a particular meaning within the context of the security environment:

Confidentiality. We want to be able to communicate or store sensitive data so that only authorized users can access it.

Integrity. We want to ensure our information, whether at rest or in transit, is not altered without authorization.

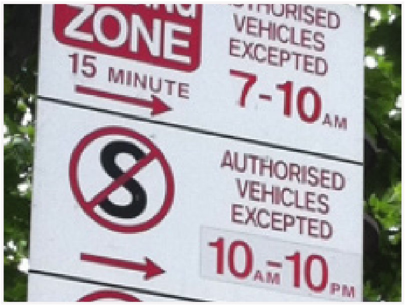
Availability. We need to ensure our business systems are ready for business whenever we need them.

Accountability. We need to be able to attribute every action with the entity that requested it.

Non-repudiation. The flip side of accountability is non-repudiation. We need to ensure an action cannot be denied after the fact.

Reliability. All of the above (and more) contribute to a system's reliability. To put it simply, a business system needs to be a workhorse we can turn to at any time with utmost confidence. A more reliable business is one that is more attractive to partners and customers. This is a competitive advantage in the marketplace.

Achieving desired outcomes



Next of course we must consider how these imperatives can be achieved. The basic recipe to produce the aforementioned desired outcomes includes four major ingredients:

Identification. We must ensure that every entity can be uniquely identified, from the end user at a desk to a web server on the other side of the planet.

Authentication. While identifying an entity is good, that identity must be verifiable to a high degree of confidence.

Authorization. We must ensure that every action is permitted by policy.

Protecting data. All businesses, large or small, have sensitive data that must be protected from disclosure and tampering. We use encryption and other techniques to protect secrets. Often, different tools and techniques are used depending on whether the information we are protecting is at rest or in transit over a network.

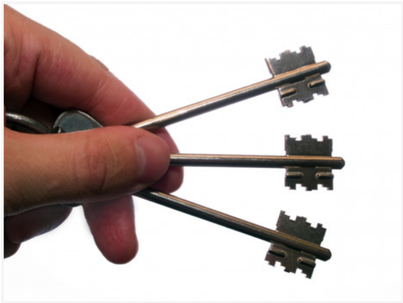
The importance of employees

As an important side note, while we will be discussing primarily technology solutions, please remember that while technology is great, the most important assets of a small business will always be the employees. Employees are the first line of defense against cyber attacks. They must be trained with basic knowledge to avoid making costly mistakes or falling unwittingly into awful traps (such as phishing attempts). And encourage them to report strange computer activity, anything that doesn't seem right; that is how many security incidents are first discovered.

Mitigating risks

There are three primary security controls that can be implemented in different ways and provide different types of value: protection, detection, and response. Detection allows us to know when a bad thing has occurred, often because a protection mechanism has failed. Even when they fail, though, we need to know. Response processes allow us to contain, halt, and then recover from bad things that we detect. All three of these things need to be adequately addressed in order to keep a business safe, secure, and resilient.

Protection measures



Some of the basic types of protections available today include:

Policies and policy management. As previewed earlier, there are many tools and mechanisms for setting and enforcing security policies, several of which are built directly into our software. For example: Users must have strong passwords; only certain employees may access this file; and so on. Of course policies are only as good as the predictable and even-handed enforcement of them.

“65% of SMBs that have a password policy do not strictly enforce it.”

- The 2016 State of SMB Cybersecurity

SOURCE: http://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html

Software updates. It is a common practice of software producers to release periodic updates to their software. Sometimes the updates fix bugs, add functionality, alleviate security defects, or address new malware threats. Many products these days can automatically download and install updates, while others still require manual intervention. Any device that uses software or firmware is potentially subject to this update requirement. Business owners need to ensure that all their systems receive an appropriate level of management. It is not sufficient to install a product and simply hope for the best.

Configurations. Most products have some degree of customizable configuration capability. This allows the user to configure the product to best serve specific needs. Configuration settings often include security features. When you purchase a new product, it pays to spend a bit of time learning the product’s features and configuration settings. Armed with a solid understanding of the available options you can optimize your configuration both functionally and with regard to the security settings.

Application software controls. When it comes to security business applications, filtering data in and out of said software is arguably one of the most useful things you can do. Many application security defects stem from the fact that software that can be tricked into misbehaving via inputting “poisonous” data. Unfortunately, filtering application data is not always an easy task. There are such things as “web application firewalls” (WAFs), which may prove useful to a business owner who cannot make changes directly to the application software.

Security products. Many security-specific products are available to help protect small businesses. These include anti-virus products, email screening tools, firewalls, and intrusion detection systems. Take time to speak to your technology advisor or managed service provider to assess what protective measures and security technologies are best suited to meet the specific needs of your business. If you do not have a professionally trained technology employee or consultant, consider it. This is not just an investment of time, it is a genuine investment in future of your business.

And one final note, all information technology providers and consultants are not necessarily information technology *security* experts. So be sure to ask what security credentials these companies and individuals can bring to the relationship with your business.

The things we protect

Every device has its own peculiarities and its own interesting features. And each needs to be protected. Not surprisingly, different types of devices require different forms of protection. Let’s consider some of these differences.

Servers. Typical small business servers (e.g., email, file servers, print servers) primarily require protection both for the data that is stored on the server and data that passes through in transit. These protections include virus screening products and spam filters, as well as basic file protection capabilities.

Desktops and laptops. Desktops and laptops are in many cases the first line of defense against unauthorized intrusion. Endpoint protection products that screen for known viruses and other malware are the most common form of protection.

Mobile devices. Smart phones, tablets, and other types of truly mobile devices often have very different security models. Endpoint protection helps, but rigorous configuration management and policy controls are often the best bet. Mobile device management (MDM) tools can help manage even a large “fleet” of mobile devices by setting and enforcing policies on various subjects such as software installation.

Networks. Network devices such as routers require careful attention when configuring. They also require software/firmware updates. The networks themselves should also be carefully protected via configuration management and policy enforcement with firewalls and the like. For remote network access, virtual private network (VPN) tools can be used to allow employees to have secure connections to a network.

Data storage and backups. Any stored user data can be compromised, including data deployed to cloud service providers and on data sharing platforms. At a minimum, regular backups need to be made of all stored data, and the data must be screened regularly for known viruses and malware. Access control protections will also go a long way to containing any infections that may occur. Ensuring that your data is backed up can make your business less vulnerable to threats such as ransomware.

Business applications. The bulk of a small business’ business happens in the main applications. This is also where some of the most pernicious attacks can occur. Protecting business applications is quite possibly the toughest part of protecting a small business that relies on them. If the applications are provided by a third party, they should be updated whenever the software provider releases updates. Further, they should be carefully configured to take advantage of whatever security features they may offer.

NOTE: This is a basic list. Please see the Resources and Planning section for further study.

Protection examples

There is a range of tools and methods used to protect servers and desktops/laptops. Some of the commonly used server protections include email scanning (viruses, malware, and attachments), activity monitoring, access control, configuration management, and user account management. For desktops and laptops, a small business may typically employ endpoint protection (viruses, malware), configuration management (software updates, security profiles), secure network connections (VPNs), and basic data protection.

Desktops/laptops need to be scanned regularly for specific signs of malicious data in files of all types. The security configuration on these devices also needs to be closely monitored in most cases. Depending on whether user accounts are controlled via a server or on the desktops themselves, account management is also highly recommended. This should include rigorous password management that requires periodic password changes, password strength rules, and so forth.

For many small businesses, these protection protocols might consist of little more than automating system and application software updates, along with some basic anti-virus/malware protection. Remember, when it comes to cybersecurity a little goes a long way.

Detection measures

In addition to implementing protection measures for their computers and computer systems, small business owners also need to be able to detect when they are under attack, regardless of whether or not the attacks succeed. Some of the most useful detection measures include the following.

Event monitoring. This is the practice of keeping a careful watch over the actions observed and noted by our systems. Most modern systems (operating systems, network components, application software) can log events as they occur. Event monitoring uses tools (as well as manual processes) to watch events for possible indications of security relevant issues (e.g., a hacker trying to break into a user's account). Event monitoring can be done by in-house staff, but there are also many security service vendors who offer this service for a fee.

Intrusion detection and prevention systems. IDS/IPS can augment traditional event monitoring by using specialized software that looks specifically for security events as they occur. IDS products traditionally alert the owner to a problem, whereas IPS products can take further action such as preventing an attacker from accessing a business system.

Threat monitoring. Threat monitoring or threat intelligence is the process of staying up to date on our adversaries' capabilities, tools, and techniques. When done well, it can help a business maintain its defenses in a meaningful way because the defenses will specifically address the known capabilities of the bad guys.

Response measures

A cybersecurity strategy without an incident response capability is not complete. Just as smoke detectors may alert you to a fire, you still need to have fire fighters at the ready to help save your business.

As you put a cybersecurity plan into place, consider firms that have experience helping small businesses respond to cyber attacks. Your information technology or managed service provider may have suggestions. What's most important is that you don't wait for a breach to have this important discussion.

The main function of a competent cybersecurity incident responder is to quickly identify the issue, to stop the attack, and to minimize damage to your business. This includes supporting investigations, recommending mitigating actions, and getting you back in business as quickly as possible.

It is vital for even a small business to conduct advanced planning to identify who you will call to respond to a security incident when it occurs. And based on the latest small business statistics, assume it will happen.

Insurance

It is clear that small businesses find their customer information, employee data, financial records, proprietary assets, and most sensitive communications on their networks. That means that what is on their networks IS their business. Yet for all of the types of insurance a small business may procure to be prepared for physical break-ins by traditional thieves, three-quarters of small enterprises have no cyber insurance to protect them from breaches of this critical information by digital criminals. In the age of Ransomware, do small businesses really want to find themselves without the resources they need to respond when these and other attacks can bring their company to its knees?

The fact is, the need for cybersecurity insurance should be considered a contemporary business necessity critical to business resilience. But all policies are not the same. There are good policies to be found, but the buyer should be very careful about the terms and conditions. There are a few key questions to ask about cyber insurance to ensure the purchase of a policy that is right for their business:

- Bundled vs. Stand alone?
- What are the policy exclusions?
- How much coverage should I purchase?
- Who is the breach response firm?

Regarding the purchase of cyber insurance, the devil is most definitely in the details or, more precisely, in the fine print. You need to procure a policy that meets the specific coverage needs of your small business. It would be rather unwise to purchase an off-the-shelf policy.

Insurance 101

There are a number of important questions that you need to ask to ensure that you get the right kind of coverage for your business.

Some of the types of losses you might consider coverage for include:

- Fraud/Criminal Activity
- Breach
- Property Damage
- Network Liability
- Investigation and Response Costs
- Business Interruption
- Extortion
- Intellectual Property
- Software & Data Loss
- Bodily Injury
- Reputational Damages

"Small businesses lose an average of $41,000 per cyber security incident. ... 60% of small businesses can expect to be hacked in a calendar year."

- Hiscox Cyber Preparedness Report 2017

SOURCE: http://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html

Be sure to look at what is not covered in your policy. For example, some fraud claims have been declined because the (insured) victim fell for a phishing attack and by mistake "consented" to wiring funds to the fraudster. Some policies do not cover victims under those sorts of circumstances.

Finally, as you make a cyber insurance procurement, be sure that you understand the insurer's compliance requirements. For example, some insurers require that customers encrypt data as a requirement for coverage. What does the insurer require if your IT system is managed by a third party? There are other examples, but the important thing is that you clearly understand all of the requirements. In the case of a breach, you don't want to find out the hard way that you won't be covered when you need it most, even though you have paid all your premiums. You also don't want to find out that your claim is denied because you misrepresented your actual security practices. If your insurance provider has a pre-qualification questionnaire, be absolutely certain that your answers accurately represent your current and ongoing security practices.

Section 4: **Cybersecurity resources**

This guidebook is intended as a general overview of the subject of cybersecurity especially as it relates to small businesses. It is notably brief and therefore cannot consider every potential threat, scenario, or the unique cyber environment of each small business. It is our hope that it will whet your appetite to learn more and more, and to take the steps necessary to at least compete on a level playing field. There are scary characters out there prowling about seeking whom they may devour. Do not allow your business to collapse out of fear or ignorance. Know the enemy, and be prepared.

In this final section, we offer a few useful resources for small business owners to learn more if you so desire.

Resources and Planning

Ann M. Beauchesne
Senior Vice President,
National Security and Emergency
Preparedness Department
U.S. Chamber of Commerce

The US Chamber of Commerce is the world's largest business federation representing more than 3 million businesses across the US—most of which are the small businesses that underpin our economy. We recognize that making the nation more cyber secure and resilient is a team effort. That is why the U.S. Chamber is pleased to partner with the Florida SBDC Network to highlight information as well as public and private sector resources to help small businesses plan to reduce cyber risk.

Since first publishing *Internet Security Essentials for Business* in 2010, the US Chamber has developed leading programs to help small business owners become more knowledgeable about cybersecurity. The *Improving Today. Protecting Tomorrow*™ campaign hosts regional cybersecurity education events with local chambers of commerce across America. You can easily find updated materials, important links, and event schedules at https://www.uschamber.com/cyber.

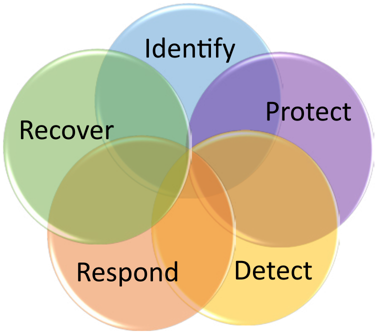
The Florida SBDC and US Chamber team with government partners as well.

The US Small Business Administration (SBA) works closely with the Florida SBDC to deliver key services to small business owner-operators. This includes providing advice on preparing for emergencies that could threaten a business—such a cyber attack or breach. In collaboration with the Federal Communications Commission (FCC), the SBA provides access to helpful cyber tips for small business as well as a tool for developing a cyber emergency plan. These resources can be found online at: https://www.sba.gov/business-guide/manage/prepare-emergencies-disaster-assistance

You may also visit the SBA Learning Center at:

https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

Meanwhile, the US Chamber has been pleased to support the National Institutes for Standards and Technology (NIST) in promoting the NIST Framework for Improving Critical Infrastructure Cybersecurity. First issued in 2014, this voluntary public-private partnership effort focuses on five key pillars for organizing business cybersecurity activities:



GRAPHIC SOURCE: Small Business Information Security: The Fundamentals, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

NIST has utilized this model to assist small business owners with publications such as *Small Business Information Security: The Fundamentals:* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

The dangers that populate cyberspace evolve every day. Unlike many business issues that come and go, cybersecurity management is now a permanent part of leading an enterprise of any size. On-going learning about new threats and a knowledge of best practices to reduce digital risk are critical to the reliability and competitiveness of a contemporary businesses. Some resources to keep you informed include:

FBI IC3. Tracking types of cyber crime and their frequency is important to alerting the national business community about growing threats, online scams, and their methods of deployment. The Federal Bureau of Investigation operates the Internet Crime Complaint Center (IC3) as a centralized resource for businesses large and small to report cyber crimes and to learn about the latest forms of attack: https://www.ic3.gov

Secure Florida. As an initiative of the Florida Department of Law Enforcement (FDLE), Secure Florida is a free, local resource for information, alerts, and recommendations for better protecting businesses and families in the online environment: http://secureflorida.org/

OWASP. The Open Web Application Security Project (http://www.OWASP.org) is a non-profit global organization aimed at helping software developers and system builders to put together secure web-based application software.

FIRST. The Forum of Incident Response and Security Teams (http://www.FIRST.org) is another non-profit global organization. Its aim is to bring together incident response organizations around the world.

Threat reports

Each year, several organizations and companies publish threat reports that summarize criminal cyber behavior and trends. Among the more prominent threat reports are:

Ponemon Institute's *Cost of Cyber Crime Study & the Risk of Business Innovation report*. This publication examines international cyber threats and assesses financial impacts over the course of the preceding 12 months. https://www.ponemon.org/library

The Verizon *Data Breach Investigations Report* (DBIR) utilizes actual breach investigation data to provide insights on the latest cyber risk. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

The Symantec *Internet Security Threat Report* (ISTR) details how simple tactics and innovative criminals impact the global cyber threat surface. https://www.symantec.com/security-center/threat-report

Related Tips

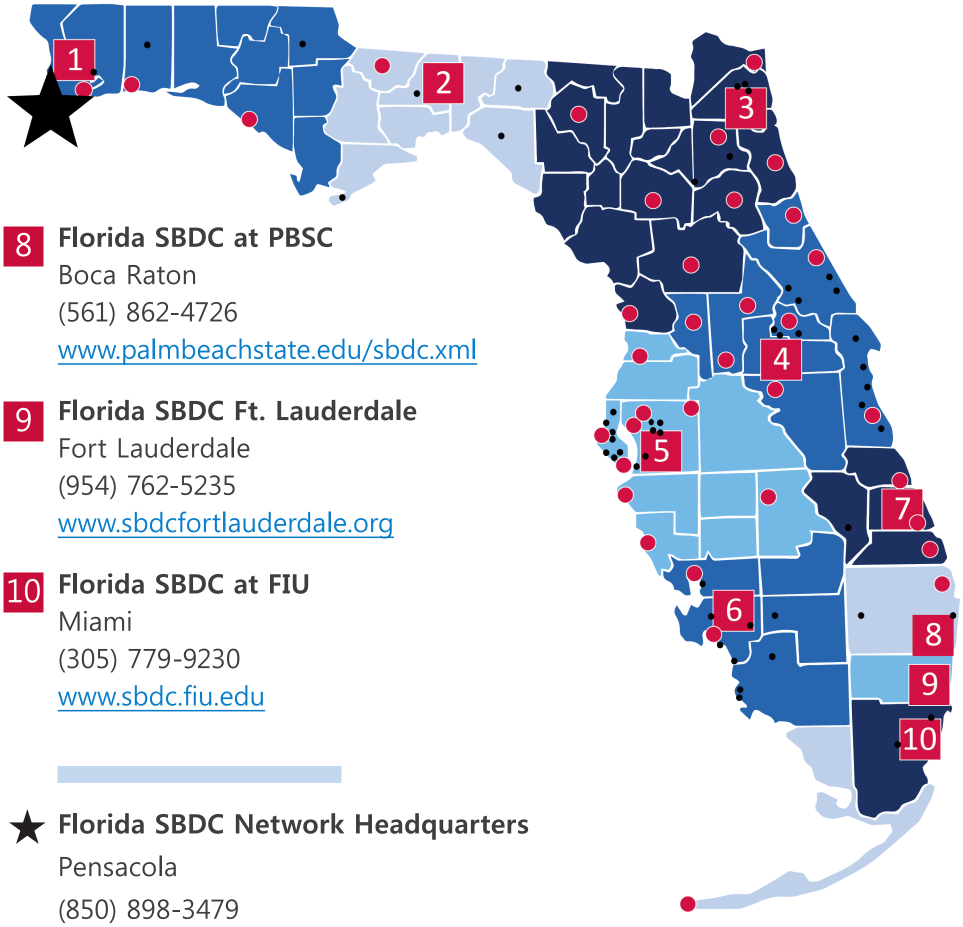
Here are few more helpful tips regarding useful resources.

- Get to know your law enforcement before you need to know them. Talk with them at a local, state, as well as national level.
- Find out what kind of assistance and resources they can provide during an incident. For example, do they have a modern forensics lab capability? Ask for a tour of their facility.
- Get to know them by name, by meeting with them.
- Look at the FBI's Infragard program to make contacts in law enforcement https://www.infragard.org.

Contact the Florida SBDC Network

Helping small businesses succeed has been the mission of the Florida SBDC Network since its inception over forty years ago. Business has changed dramatically during this time, however the Florida SBDC's commitment to meet the complex and ever-changing needs of entrepreneurs and small businesses has remained the same. From building business plans and supporting revenue growth, to better management of small business challenges such as cyber risk, Florida SBDC consultants stand ready to help.

State designated as "Florida's principle provider of small business assistance," the Florida SBDC Network has more than 40 offices from Pensacola to Key West to serve the needs of Florida's business community. Contact one of the key points of contact below to start on your path to cyber readiness today.



1 **Florida SBDC at UWF**
Pensacola
(850) 474-2528
www.sbdc.uwf.edu

2 **Florida SBDC at FAMU**
Tallahassee
(850) 599-3407
www.sbdcfamu.org

3 **Florida SBDC at UNF**
Jacksonville
(904) 620-2476
www.sbdc.unf.edu

4 **Florida SBDC at UCF**
Orlando
(407) 420-4850
http://sbdcorlando.com

5 **Florida SBDC at USF**
Tampa
(813) 905-5800
www.sbdctampabay.com

6 **Florida SBDC at FGCU**
Fort Myers
(239) 745-3700
www.fsbdcswfl.org

7 **Florida SBDC at IRSC**
Fort Pierce
(772) 462-7296
www.irscbiz.com

8 **Florida SBDC at PBSC**
Boca Raton
(561) 862-4726
www.palmbeachstate.edu/sbdc.xml

9 **Florida SBDC Ft. Lauderdale**
Fort Lauderdale
(954) 762-5235
www.sbdcfortlauderdale.org

10 **Florida SBDC at FIU**
Miami
(305) 779-9230
www.sbdc.fiu.edu

★ **Florida SBDC Network Headquarters**
Pensacola
(850) 898-3479

→ **FloridaSBDC.org/Cybersecurity**

Glossary of Key Terms

Botnets: a network of computer robots, used to perform some malicious action en masse.

Business Email Compromise (BEC): a seemingly legitimate internal email that is designed to trick users to disperse funds or to disclose financial or other sensitive information.

Denial-of-Service (DoS): a type of cyber attack made from a one computer connection that denies legitimate users from utilizing the internet connected services of the victim by overwhelming the targeted system with excessive information or requests.

Distributed Denial of Service (DDoS): a type of DoS attack that utilizes many botnet-controlled computers—often located in many parts of the world (distributed)— to attack another computer or computer system in order to deny service.

Encrypted: the process of encoding information or data to help prevent unauthorized access.

Hardware: physical components of a computer, smartphone or other electronic system.

Internet of Things (IoT): the growing network of Internet-connected devices, such as home security systems, automobiles, and kitchen appliances, which are increasingly being targeted for malicious attacks.

Malware: malicious software that is developed with the express purpose of altering, manipulating, incapacitating or otherwise damaging computers or electronic systems.

Phishing: a type of social engineering attack designed to lure the victim into doing something ill-advised on email, such as execute an attachment, click on a link, or unwittingly give away sensitive information.

Ransomware: a malware tool used by cyber criminals to encrypt (lock-up) a victim's data rendering it inaccessible unless a ransom payment is made to restore access.

Sabotage: any deliberate malicious act against a victim's computer or computer system.

Social Engineering: a method utilized by nefarious cyber actors to trick or manipulate humans into taking actions on digital platforms in order to steal information, money, etc.

Software: programs and other operating instructions and data installed onto a computer, smartphone or other electronic system.

Spoofing: a cyber crime tactic in which the attacker poses as a legitimate user or known entity to gain access to information or trust from other legitimate users.

Notes

Notes

AMERICA'S SBDC FLORIDA
Helping Businesses Grow & Succeed

The Florida SBDC Network Byte-Size Program:

Cybersecurity Basics for Small Business

The Florida SBDC Network is a statewide partnership program nationally accredited by the Association of America's SBDCs and funded in part by the U.S. Small Business Administration, Defense Logistics Agency, State of Florida, and other private and public partners, with the University of West Florida serving as the network's lead host institution. All opinions, conclusions, and/or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of the SBA or other funding partners. Florida SBDC services are extended to the public on a nondiscriminatory basis. Language assistance services are available for individuals with limited English proficiency.

→ FloridaSBDC.org/Cybersecurity

State Designated as Florida's Principal Provider of Business Assistance [§ 288.001, Fla. Stat.]