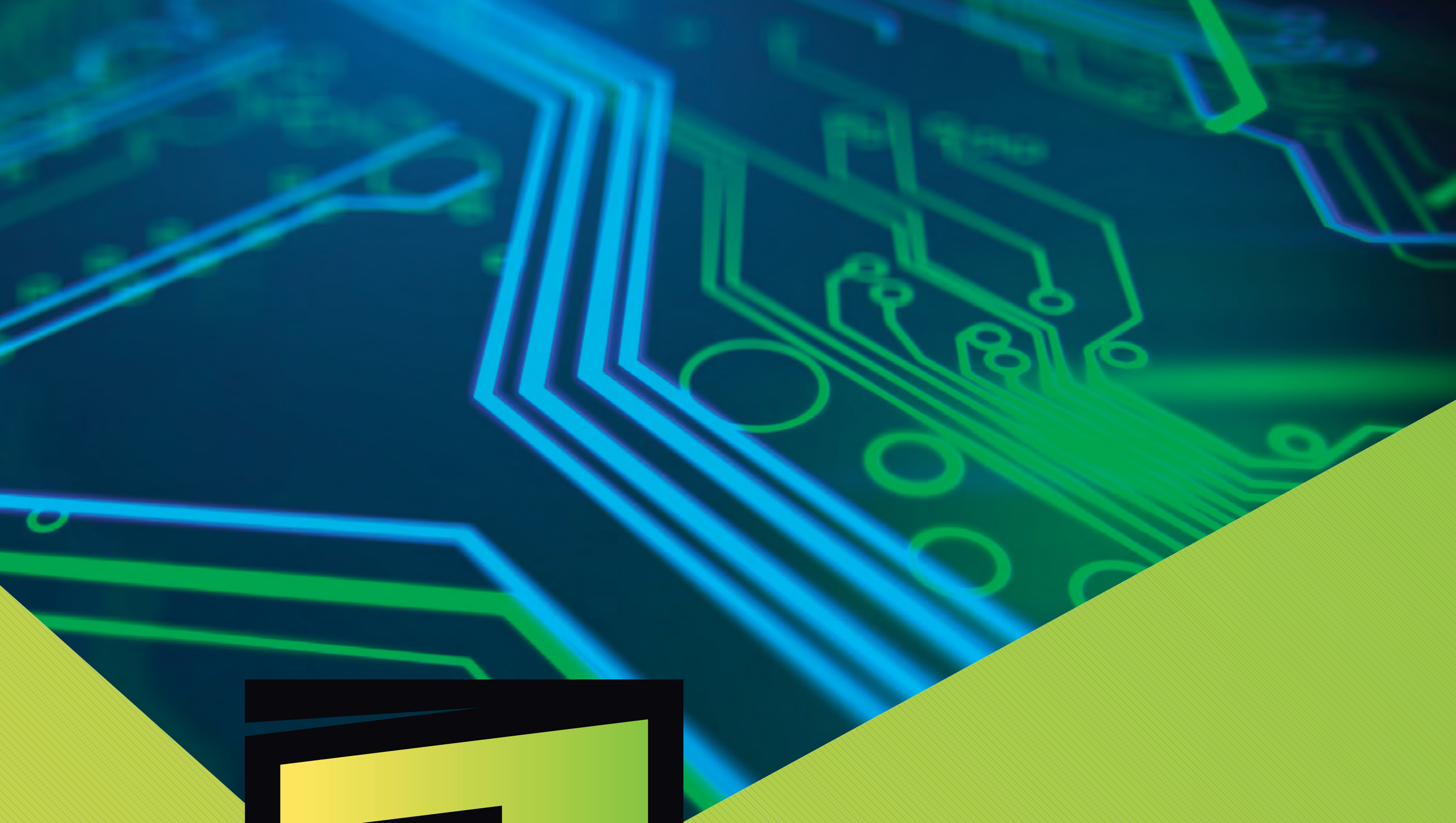


CYBER DEFENSE FOR SMBs

a beginner's guide to cybersecurity provided by CYBER FLORIDA

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

Dear reader,

Cybersecurity—a word that only entered our collective lexicon about 30 years ago—is now constantly on the forefront of the daily news cycle. State-sponsored attacks on our elections, massive data breaches affecting major international corporations with millions of customers, and even theft of intellectual property from our leading universities have all made headlines in the past year.

What doesn't make headlines, though, are the thousands of cyberattacks perpetrated against small and medium-sized businesses (SMBs) throughout the United States each year. The *2018 Verizon Data Breach Investigation Report* found that 58% of malware attack victims were small businesses, and the Ponemon Institute's *2018 State of Cybersecurity in Small and Medium-Sized Businesses* reported that 67% of small businesses experienced a cyberattack in 2018.

Small businesses are targeted by cybercriminals precisely because they are small. Criminals know these businesses typically lack the financial resources necessary to employ state-of-the-art cyber defenses, but still trade in the same consumer data and intellectual property as larger businesses that can afford to invest more in cybersecurity. For a cybercriminal, the decision is easy.

> **47% of SMBs** say they have no understanding of how to protect their companies from cyberattacks.
>
> Ponemon Institute

Our goals with this guide are to help you think of potential vulnerabilities within your business so that it can avoid becoming a victim of this troubling trend and, if it is targeted, to help you identify qualified resources to assist you in responding to, and recovering from a cyberattack with your business intact.

Cyber Florida has called upon cybersecurity experts from academia, private industry, government, and the military to help create this easy-to-follow, plainly written guide on achieving adequate security with limited resources. We hope that it will empower you to take control of your business's data and help you identify the most cost-effective cybersecurity investments to address your business's specific needs.

This guide is supplemented by a resource-rich website, cyberflorida.org/SMB, that offers tools, links, and advice to help you stay on top of the ever-evolving world of cybersecurity. You can also sign up to receive Cyber Florida emails that will alert you to the latest news and events hosted by Cyber Florida as well as our academic, industry, and government partners.

Congratulations on taking this step to improve your business's cybersecurity!

Sincerely,

Sri Sridharan
Director, Cyber Florida: The Florida Center for Cybersecurity

This guide is made available by the Florida Center for Cybersecurity for general educational purposes only and should not be used in lieu of obtaining competent legal advice from a licensed attorney and/or cybersecurity professional with the sufficient expertise necessary to address your organization's specific needs. Use of this guide does not create any special or fiduciary relationship between you and the Florida Center for Cybersecurity or the University of South Florida.

CYBER DEFENSE FOR SMBs

Table of Contents

Part One: Threats

Part Two: Best Practices

Part Three: Crisis Management

Published by Cyber Florida
Sri Sridharan, *Director*

Principal Writer
Guise Bule, *Founder of Secjuice.com*

Contributors
Ronald Sanders, PhD
COL (RET) John McLaughlin
Mark G. Clancy
Daniel Eliot
Steve Berlin, Esq.

part one

Threats

Who Perpetrates Cyberattacks?

Cyberattacks against small, medium, and large businesses are on the rise. Most likely, you just read about a major cyberattack within the last month. These days cyberattacks are pervasive, compared to just a decade ago, and cybercriminals do not confine themselves to attacking only large businesses. They increasingly target small and medium-sized businesses because they know these types of businesses are less likely to have sophisticated security infrastructure in place compared to a larger business.

You may think your business is too small for a cybercriminal to bother with but, to cybercriminals, a small business may be an easy and valuable target.

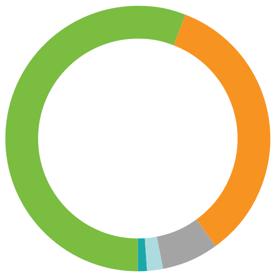
Who is behind these cyberattacks? According to most cybersecurity professionals and the latest industry reports, the vast majority of attacks are caused by what we call 'malicious outsiders.' These are criminally minded people who have no direct connection to your business.

The motivations driving these individuals are considered malicious because they primarily want to attack your business for financial gain, regardless of the damage it could cause to you and your customers. Most malicious outsiders are criminals who set out to infiltrate your business to make money, and as a business owner, these are the cyberattacks that you can affect you more than any other.

Other types of attackers include hacktivists—people who target businesses involved in controversial affairs—and malicious insiders such as disgruntled current or former employees with an ax to grind against the company.

There is also a chance that state-sponsored operators (i.e., foreign spies) will attack your business for espionage-based reasons; this should be a significant concern for small businesses that work as government contractors or deal with confidential intellectual property.

Let's take a closer look at who these cybercriminals are.

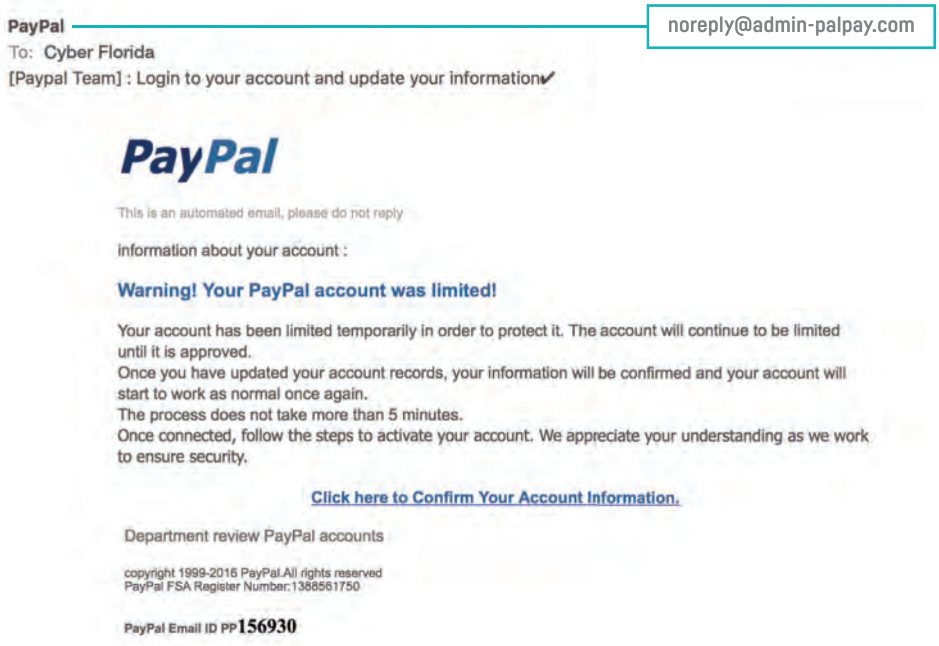


BREACHES BY SOURCE

56%	34%	7%	2%	1%
Malicious Outsider	Accidental Loss	Malicious Insider	Hacktivist	State-Sponsored

Gemalto 2018 Breach Level Index Annual Report

Always examine the sender field. In this case, the email was actually sent from a malicious account.



noreply@admin-palpay.com

PayPal
To: Cyber Florida
[Paypal Team] : Login to your account and update your information✔

PayPal

This is an automated email, please do not reply

information about your account :

Warning! Your PayPal account was limited!

Your account has been limited temporarily in order to protect it. The account will continue to be limited until it is approved.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.
The process does not take more than 5 minutes.
Once connected, follow the steps to activate your account. We appreciate your understanding as we work to ensure security.

Click here to Confirm Your Account Information.

Department review PayPal accounts

copyright 1999-2016 PayPal.All rights reserved
PayPal FSA Register Number:1388561750

PayPal Email ID PP156930

Many phishing emails start with bad news.

"Warning! Your PayPal account was limited."

The first indication is that this is an email from PayPal. However, there are several clues that tell us that this is a phishing email.

- Poor spelling and grammar
- Urgency
- Legitimate companies rarely ask you to 'click here' to confirm anything

When in doubt, navigate to the website in question without clicking a link.

Hackers - A hacker is an unauthorized intruder who tries to break into your businesses network, databases or systems, primarily for financial gain, but a rare few will hack you for fun. Hackers fall into the malicious outsider category, and they have a big box of tricks that they can use to infiltrate your business, ranging from specially created tools that exploit known or unknown vulnerabilities in your IT infrastructure to simply guessing your passwords.

Hacktivists - A hacktivist, also a malicious outsider, is a hacker with a cause. They will try to infiltrate your business because you engage in an industry or practice they disagree with, so much so that they are willing to commit a crime to punish you and your business. Often, a hacktivist will deface your website with political messaging and contact your customers to tell them of your supposed wrongdoing. They may also steal and release your data, but it's less likely that they will do so for their own financial gain and more likely to affect things such as your image or customer confidence.

in their words

"Companies spend millions of dollars on firewalls, encryption, and secure access devices, and it's money wasted because none of these measures address the **weakest link in the security chain: the people who use, administer, operate and account for computer systems** that contain protected information."

–Kevin Mitnick
Chief Hacking Officer, KnowBe4

Phishers - Phishers also fall into the malicious outsider category. They are cybercriminals who send 'phishing' emails, so named because they are designed to *fish* for login credentials and other information. They do this by posing as a legitimate online service that you may use and emailing you from that fake service, usually with some type of account maintenance alert message.

Phishers are the people who send you those urgent password reset emails while pretending to be from your financial institution. One big danger of phishers is that, even with constant training, their emails can sometimes fool the best of us.

What is Spoofing?

Spoofing is a malicious practice in which an email is sent from an unknown source disguised as a source known to the receiver.

Phishers are probably the most common threat and the most common kind of cyberattack that your business is likely to encounter. They are also among the most difficult to stop because phishers use sophisticated tactics, typically pretending to be somebody you know and usually emailing from an address that you recognize. They do this by spoofing the sender's address, and typically, their emails direct you to an online login that is probably doing a great job of posing as a legitimate online service but is really a false front designed to capture your login credentials.

Malicious Insiders - More often than not, malicious insiders are disgruntled employees intent on causing damage to your IT infrastructure, typically sabotage as opposed to stealing data for profit. Sometimes malicious insiders are agents of corporate espionage who have been promised a job by one of your competitors if they leave with your customer list, for example. It is quite common for less sophisticated malicious insiders to be caught after their wrongdoing, as they typically leave a trail of motivation and evidence, but this is not always the case with the more sophisticated malicious insiders.

Quick Wins for email security.

WHEN IN DOUBT, THROW IT OUT.
BE EXTRA CAUTIOUS WHEN IT COMES TO EMAIL.

- Require strong, unique passphrases on email accounts
- Turn on two-factor authentication
- Do not use personal email accounts for company business
- Employees should know not to open suspicious links in email, tweets, posts, online ads, messages, or attachments – even if they know the source. Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email
- Learn more: ***https://www.ic3.gov/media/2017/170504.aspx***

What Are the Four Main Types of Attacks?

There are four main types of cyberattacks, known as the Four Ds: *Data loss, Disruptive, Destructive, and Disinformation*. Let's look at these types of attacks in more detail to familiarize ourselves with the nature of threats, so that we may better understand them and defend against them.

Data Loss or Exposure - Data loss is quite possibly the most damaging cyberattack, depending on the importance of your data. If you lose your customers' personal, financial, or other data because of a cyberattack, your business likely will suffer from a significant reputation loss in addition to the potential legal and financial liabilities that go along with a data breach. In many cases, organizations that suffer a major data loss become the subject of legal action against them by those affected, potentially resulting in multi-million-dollar compensation payouts and fines, depending on where the company is based.

The average cost for each lost or stolen record containing sensitive and confidential information **in the U.S. is $233—the highest in the world.**

2018 Cost of a Data Breach Study by the Ponemon Institute

Disruptive - This type of attack is designed to disrupt or impair your business's ability to function in some way. A prime example of this kind of attack is a ransomware attack. In a ransomware attack, the attackers encrypt your business's data and demand a (usually small) ransom to decrypt it, severely restricting your ability to operate as a business until the ransom is paid. This type of attack can last days or weeks, and often the only way to deal with the issue effectively is to pay the ransom. Another form of disruptive attack is a Distributed Denial of Service, or DDoS (pronounced dee-doss) attack, in which the attacker uses multiple computers to send an overwhelming amount of traffic to your website, causing the site to crash and disrupting your business operations.

Destructive - Typically, malicious insiders or hacktivists deliver destructive attacks, which are designed to harm your business by damaging your IT infrastructure in some way. A destructive attack could be as simple as deleting your data and backup data, or as extensive as wiping all computers of their applications and software—causing your operations to seize—or defacing your public-facing websites with embarrassing messages. Any element of your business that is connected to the internet can be affected by an attacker bent on damaging your business.

Disinformation - Disinformation attacks against your business spread false information about your activities and employees to inflict reputation, financial, and even legal damage. Malicious disinformation about your business can spread quickly through many different social and digital channels, much faster than you can counter it or have it removed. A sustained campaign can inflict serious damage on your business even if none of it is true, and in many cases, you have no real idea of who is behind it—competitors or malicious insiders.

How Are Attacks Carried Out?

Before talking about how cyberattacks are carried out, let's talk about the "attack surface," which is a professional term used to describe the collection of devices, hardware, and software that compose your IT infrastructure. The attack surface includes all mobile devices, endpoints (PC's and laptops), servers, routers, printers, websites, databases and data storage, and web applications. Any device, hardware, and software application that connect to your business network can serve as the point of entry for an attacker and are part of the attack surface.

Because the average business's attack surface is quite large, there can be numerous avenues for a hacker to find a way into your IT infrastructure. While a lot of cyberattacks are opportunistic—occurring when a hacker finds a convenient vulnerability in your IT infrastructure that makes it easy to hack—others are much more calculated events. More advanced attacks involve hackers developing their own programs to bypass your security, install malware onto your system, and give them unrestricted backdoor access to your data and IT infrastructure.

Ultimately, any connected device is a potential infiltration point for a hacker, but let's take a closer look at the most common points of entry to your business.

a case study

The Connected Fish Tank: In 2017, particularly clever hackers were able to access the network of a North American casino through its fish tank. The tank had sensors to regulate temperature, food, and cleanliness, which were connected to a PC. The hackers compromised the tank and accessed other areas of the network from there. A small amount of data was sent to a device in Finland before the casino's cybersecurity platform discovered the breach and stopped the threat.

Phishing Attacks - Phishing is probably the most common type of cyberattack against businesses and involves the extraction of personal information and login credentials from your users by means of deception. Phishing emails are designed to look like they come from a reputable service provider—financial institutions and streaming services are popular choices for impersonation because they are so widely used—and often include a reasonable yet urgent request to attend to some account issue such as an expired credit card. Should you click the link in a phishing email, it will take you to a website that looks almost identical to the service provider's actual site, hoping to trick you into entering your login details or other personal information.

These sophisticated attacks can fool even the savviest tech users. It was a phishing attack targeting a top official in the Democratic party that led to the release of 60,000 private emails in the runup to the 2016 presidential election. More commonly, though, these attacks are used to prey upon businesses and individuals for financial gain.

Phishing emails may also contain file attachments intended to infect your computer or mobile device with malware. Sometimes they will try to gain your trust by including some personal information about you that makes you more inclined to believe the email is legitimate, a tactic known as "pretexting." Using these tools of deceit, cybercriminals extract millions of dollars a year from small, medium, and large businesses across the country.

Social Engineering Attacks - Social engineers practice the art of infiltrating your systems, buildings, and data by exploiting human psychology instead of using technical hacking techniques. Like phishing, this kind of attack is hard to defend against because it attacks the individuals in your business to gain access to your systems rather than attacking the actual system itself. Rather than spending time searching for a vulnerability in your IT infrastructure, an attacker instead contacts your employees posing as a support technician or pretending to be from another department, with the goal of tricking the employee into sharing login credentials or other sensitive data.

A major concern with social engineering is that you could have all the latest cybersecurity tools in place to protect your business and still fall prey to these techniques because the weakest link in any organization's attack surface is people. Social engineers can be incredibly effective at getting passwords out of your unsuspecting employees, and once they have that password, they can access your system while appearing to be a legitimate user.

in their words

"**A single spearphishing email carrying a slightly altered malware can bypass multimillion-dollar enterprise security solutions** if an adversary deceives a cyber-hygienically apathetic employee into opening the attachment or clicking a malicious link and thereby compromising the entire network."

–James Scott
Senior Fellow, Institute for Critical Infrastructure Technology

Malware Attacks - The two biggest sources of malware infections for businesses are employees visiting websites and clicking on malicious links and employees opening phishing email attachments. Once malware gets a foothold, it can be difficult and expensive to get rid of.

Examples of malware are:

Remote Access Trojans - Allows the attacker backdoor entry into your systems.
Ransomware - Designed to encrypt all your data until you pay a ransom.
Spyware - Designed to log your keystrokes to gather data such as passwords.
Adware - Designed to expose the victim to potentially malicious advertisements.
Worms - Designed to self-replicate, spreading far and wide without user interaction.
Viruses - Designed to infect other legitimate files, making cleanup difficult.

These are the primary malware strains, although there are far more exotic and hybrid malware strains to be found. Depending on the malware strain, it can be very difficult to get rid of, and some strains of malware, such as rootkits, may be impossible to get rid of even when you completely wipe your computer and reinstall your operating system and software.

Point-of-sale (POS) Intrusions - The POS system that your business uses to process customer transactions has long been a high-value target for cybercriminals, and digital point-of-sale cash registers are frequently infected with malware designed to steal your customers' credit card numbers. POS intrusion attacks affect even the biggest businesses. Earlier this year the clothing retailer Eddie Bauer, fast food merchant Wendy's, and the Kimpton Hotel Group were all victims of this type of attack.

Commonly, POS systems are breached via the remote access points that their providers use to manage and technically support the terminals; other times hackers gain access because the POS system is poorly configured, using either the default password or an easy-to-guess password. Once a hacker has access, they can silently siphon off your customers' transactional and credit card data for months, years, or as long it takes for you to detect them.

The biggest breaches ever caused by phishing attacks

that we know of...

2014, eBay
A phishing attack garnered the credentials of as many as 100 employees, leading to the breach of 145+ million customer records.

Cost: Estimated $200 million in sales revenue.

ebay™

2014, Sony Pictures Entertainment
Attackers sent Sony's top executives fake Apple ID verification emails, then used the stolen credentials to gain entry to Sony's network, crippling the company's computer networks and stealing 100+ terabytes of data.

Cost: Reported $35 million to repair its IT infrastructure.

SONY
PICTURES

Quick Wins for point of sale systems.

HACKERS ARE OFTEN FINANCIALLY MOTIVATED. DON'T MAKE IT AN EASY PAYDAY.

- Create unique, strong passphrases
- Separate user and administrative accounts
- Keep a clean machine: update software regularly
- Avoid web browsing on POS terminals
- Use antivirus protection
- Learn more: ***https://www.pcisecuritystandards.org/merchants/***

We will take a closer look at POS breaches later on in this guide when we review the Target data breach case study, in which cybercriminals harvested the details of 40 million debit and credit card accounts. In that breach, the attackers were in Target's systems long enough to harvest the personal details of approximately *70 million individuals*, in addition to the card data.

System Vulnerabilities – A system vulnerability is a flaw or weakness in the system that leaves it vulnerable to an attack or exposes data. System vulnerabilities can arise from a variety of causes, including a design flaw in the hardware or software, a manufacturing defect, failure to apply updates and patches, use of pirated or illegitimate software, and misconfiguration. Regardless of the cause, system vulnerabilities are obvious infiltration points for hackers, who see them as convenient gateways into your systems that often do not require much work on the hacker's part. A talented (or lucky) hacker may find that you have desktop operating systems that are not up to date, application software that has not been upgraded, or a legitimate remote access point intended for support technicians that has been left unsecured.

2015, Pentagon

Attackers used a phishing attack to gain access to the Pentagon's Joint Staff unclassified email system.

Cost: System shut down for two weeks, 4,000+ military and civilian personnel affected, costs of repairing the system unknown.

2015, Anthem

Five employees opened a phishing email and unknowingly downloaded keystroke logging software, leading to the breach of 80+ million customer records.

Cost: Estimate $100 million

Anthem.

Windows 7, the most popular operating system in the world, **has 996 known vulnerabilities**.

–cve.mitre.org

System vulnerability patches are one reason why it is so important to keep your operating systems, software, and firmware regularly updated; these updates often contain *known vulnerability* patches to fix holes in your systems. If you fail to timely update your systems, or apply these update patches, any hacker who notices will be able to quickly research known vulnerabilities for your out-of-date software that they can then use to gain access to your systems.

Even if you do keep everything updated, system vulnerabilities can still pose a threat through what is known as a "zero-day attack," when a hacker discovers a previously unknown vulnerability and acts quickly to take advantage of it before a patch is issued. Fortunately, zero-day attacks against a small business are uncommon; these types of attacks are typically reserved for high-value targets for two reasons. First, the hacker must invest time and resources to create the attack, so they reserve their efforts for targets with the highest potential payoff. Second, once exploited, the vulnerability may be detected and mitigated, limiting the window to take advantage of the vulnerability.

WANNACRY AND NOTPETYA

In May 2017, the world was struck by **WannaCry**, a ransomware attack that quickly spread to nearly 150 countries and caused more than $4 billion in damages, including crippling the United Kingdom's National Health Service, infecting 16 hospitals. This attack was surprising not only because of its massive scale but also because it leveraged a vulnerability in older Microsoft Windows operating systems that had been patched a full 91 days prior. Worse than that, about a month later a similar ransomware attack, known as **NotPetya**, was launched that took advantage of the same vulnerability. That attack cost shipping giants Maersk and FedEx an estimated $600 million combined.

a case study

advice from the experts

Mark G. Clancy
Cyber Florida Board Member, CISO, Sprint

Small Changes Make a Big Difference

Electronic mail is one of the ways businesses of all sizes keep in contact with customers and engage to close deals. Criminals know this and have targeted email accounts directly by stealing passwords or sending fake emails in which they pretend to be a party to a transaction and either change instructions for a payment or collect sensitive information such as W-2 data. Collectively, this is known as a "business email compromise," and the FBI estimates that in the last 5 years this has cost businesses over $12 billion dollars in losses. No business is too small to be targeted by criminals with this type of crime. In the U.S., the average lost was $71,000.[i]

One way criminals compromise the business or customer email account by stealing passwords through malware, followed by impersonating one of the senders and changing some detail of the transaction. This is particularly rampant in real estate transactions where, for example, a fake instruction is sent asking the buyer to wire money to an account instead of using a paper check. The account sent by the fraudster in the emails is of course not the right destination for the transaction. This is not the only type of scam; another common method is to use a compromised or spoofed account to ask for information such as tax records or personal data while one of the parties is traveling, for example. This may cross over into telephone calls where the criminal impersonates one of the parties. Since the criminal had access to the email account, they likely have context information about the transaction or what is going on in your company. Criminals may also use email to send malicious software, links, or messages designed to collect sensitive information or may harvest information from your social media posts.

What can I do to make my business more resilient to these kinds of attacks?

1. Limit what you post publicly on social media about major transactions or business travel when possible.
2. Turn on stronger two-factor authentication for your email account.
3. Use either a standalone one-time password generator application (e.g. Duo, Authy, Saaspass, etc.) or a Universal Second Factor (U2F) authentication hardware token. When Google implemented a U2F hardware token for their staff, they had zero compromised email accounts across 85,000+ users.[ii]
4. Don't use text-based second-factor authenticators if better options are available.
5. Setup a secondary pin/password/code with your mobile carrier to require additional information to replace your SIM card or move your phone to another carrier.[iii]

Also, be careful to look at how your email provider resets passwords/credentials as, often, mobile phone numbers are used for backup. Criminals have been going after victims' mobile phones by deceiving their mobile phone carrier and asking for a replacement phone or SIM card, which is called SIM swapping. Criminals do this so they can intercept text messages and telephone calls to misdirect transactions or answer security challenges either by text or voice.

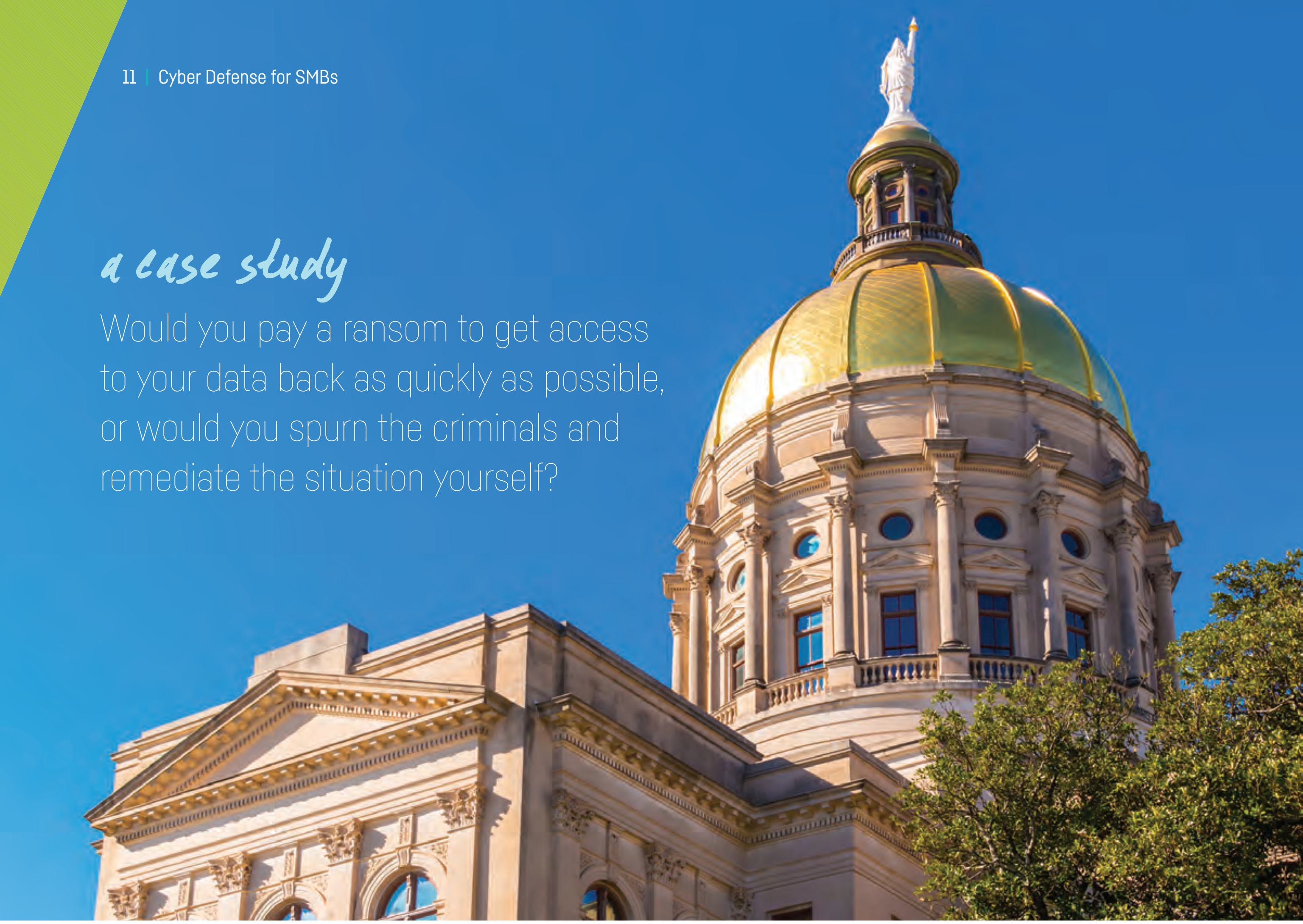
advice from the experts

Small Changes Make a Big Difference

[i] https://www.ic3.gov/media/2018/180712.aspx

[ii] https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/

[iii] https://www.digitaltrends.com/mobile/sim-swap-fraud-explained/



a case study

Would you pay a ransom to get access to your data back as quickly as possible, or would you spurn the criminals and remediate the situation yourself?

Atlanta Ransomware Attack

The ransomware attack that hit Atlanta is worth talking about because it was so disastrous in every sense that it gives us a good idea of the dynamics at play when an organization is hit by a cyberattack. While in this case a whole city was affected, these same kinds of attacks plague small businesses every day across the U.S.

In March 2018, attackers infected the City of Atlanta's IT systems with a strain of ransomware called SamSam, causing city services to grind to a halt. Suddenly, residents could not pay for essential services like water, police efficiency plummeted as they reverted to pen and paper, and the city could not collect parking fines. The cybercriminals demanded the city pay a ransom of $50,000 in bitcoin, prompting internal debates about the ethics of paying the ransom.

The SamSam malware strain is only the latest actor in sustained ransomware campaigns against public services, including critical systems like the 911 dispatch system. These unscrupulous criminal actors know that authorities will pay quickly to restore such essential services, and the criminals are getting bolder.

Would you pay a ransom to get access to your data back as quickly as possible, or would you spurn the criminals and remediate the situation yourself? Sadly, many businesses decide to pay the ransom because they lack the resources to recover from such an attack on their own. What's worse, many pay the ransom and do not report the incident out of embarrassment. In these cases, it is important to remember that even a small business has hundreds, possibly thousands, of potential access points to secure, and

> “Ransomware is unique among cybercrime because in order for the attack to be successful, **it requires the victim to become a willing accomplice after the fact.**”
>
> –James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology

criminals only need to find *one* weak spot. There is no shame in being victimized by these sophisticated and relentless criminals.

The attack on Atlanta, however, was playing out in the public domain, and officials felt that paying the ransom would invite future copycat attacks by criminals expecting a quick payout. They opted not to pay the ransom.

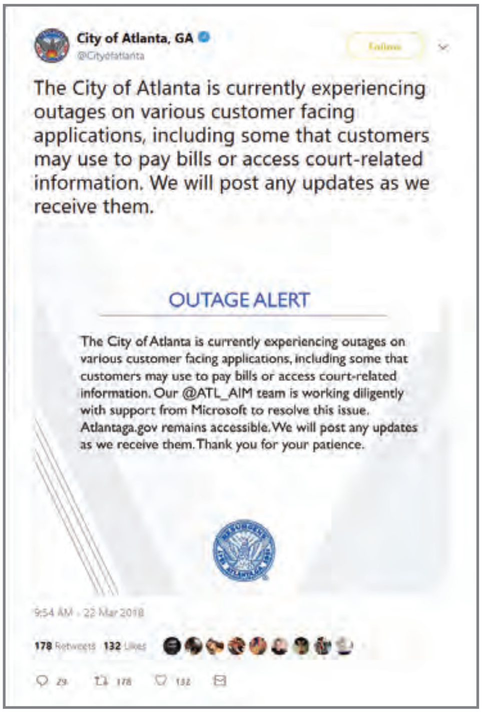
In the end, **the City of Atlanta spent a reported $2.7 million in emergency funds** to properly respond to and recover from the attack, the bulk of the money going to external cybersecurity contractors and incident response consulting. In a June 2018 city budget meeting, officials requested an additional $9.5 million to address the remaining damage.

Law enforcement typically advises one should not pay a ransom because it encourages the criminals, but it’s not always a clear-cut decision. For many businesses, a sustained outage of their IT can have serious consequences and emergency spending on cybersecurity cleanup efforts—which average $690,000 for a small business and over $1 million for a medium-sized enterprise—can drive them to the point of bankruptcy.

Criminals typically set the ransom at an amount they think their victims can afford, so for a lot of small businesses, the choice is between paying a few thousand in ransom or significantly more on remediation costs.

In the case of the City of Atlanta, who decided not to pay, they will undoubtedly benefit over the long term because paying professionals to remediate the situation is effectively an investment in their future cyber defense. Other criminals now know that not only is the city unwilling to pay a ransom, but also that it will be much harder to penetrate the city’s newly improved defenses.

Whichever way you look at it, and however you decide to deal with the ransom, an attack like this can cost you a significant amount of money and can even drive your businesses into bankruptcy. Fortunately, there are steps you can take and small investments you can make now to help prevent these types of attacks, which will be reviewed later in this guide.



City of Atlanta, GA
@Cityofatlanta

The City of Atlanta is currently experiencing outages on various customer facing applications, including some that customers may use to pay bills or access court-related information. We will post any updates as we receive them.

OUTAGE ALERT

The City of Atlanta is currently experiencing outages on various customer facing applications, including some that customers may use to pay bills or access court-related information. Our @ATL_AIM team is working diligently with support from Microsoft to resolve this issue. Atlantaga.gov remains accessible. We will post any updates as we receive them. Thank you for your patience.

9:54 AM - 22 Mar 2018

178 Retweets 132 Likes

a case study

Target HVAC Breach

The now-famous Target data breach is a good example of an organization that was infiltrated by cybercriminals through a third-party vendor, in this case an HVAC vendor that served several Target locations across the country.

It is likely that the vendor had access to Target's networks so that they could monitor temperatures in the stores where they had installed air conditioning units and technically support those units remotely if needed. Remote access may save the vendor unnecessary onsite visits, but often vendors don't inform their customers that they have installed a remote access backdoor into the system, and customers don't always think to ask. Don't make the same mistake.

Once the attackers had infiltrated the HVAC vendor, they started the attack using that vendor's network access to infiltrate Target, eventually managing to install malware on Target's POS devices, which were gathering credit card numbers and customer details from live transactions. In this way, the criminals managed to gather approximately 40 million debit and credit card numbers together with the personal information of 70 million individuals.

Thus far, the Target breach has cost more than $100 million and counting...

At the time, this was the biggest data breach in history, and Target had to pay approximately $17 million to those affected. The breach cost is estimated to be $100 million in lost reputational value, lost business, and cyberattack cleanup costs.

While this was a noteworthy breach, it is important to remember that this is a very common problem. Some vendors install remote access without notifying the customer and without taking the time and care to ensure that the connection is secure; it's a major problem that plagues the retail space.

One reason this continues to be an issue is that there are no universal security standards, no best practice processes or controls that vendors can follow when they need remote access to a client's system. Ultimately the obligation is on the client—you and your business—to ask the right questions when employing a third-party contractor, even one that seemingly has nothing to do with your business processes.

It's critical to make sure that your vendors are not only cybersecurity aware, but also proactively protecting the digital connections that they have with you and your business. Make sure they have security practices, processes, and systems in place to protect you and your data before trusting your business to them.

"Third-party error" was named as the root cause of **43% of SMB data breaches in 2018**.

Ponemon Institute

Quick Wins quick wins for third-party vendors.

DO YOUR DUE DILIGENCE, GET IT IN WRITING, AND MONITOR COMPLIANCE.

- Spell out your privacy and security expectations in clear, user-friendly language to service providers
- Understand how their services work and to what you are giving them access
- Build in procedures to monitor what service providers are doing on your behalf
- Review your privacy promises from the perspective of a potential service provider
- Spell out expectations and scope of work in a formal agreement/contract
- Learn More: ***https://bit.ly/2PIUbWv***

Third-Party & Supply Chain Risks

It's not just your security that you have to worry about; you should also consider threats from third parties, usually your partners, and the supply chain. A supply chain cyberattack is when criminals infiltrate your IT systems through a partner or provider that already has access to your systems and data.

The bad news is that these attacks are on the rise and are becoming increasingly common as a preferred infiltration route for attackers. Both Target and Equifax were breached by cyberattacks that infiltrated them through their vendor supply chains. To make matters worse, the supply chain for most organizations can be so complex that it makes identifying and mitigating supply chain cybersecurity threats hard for even the best cybersecurity teams.

It is this complexity that makes our supply chains so fraught with cyber risk, and when it comes to third-party and supply chain risks, security is not just a technology problem; it's also a people, process and knowledge problem.

The more people and partners you add to the supply chain mix, the greater the chance that you will become the victim of a cyberattack via that channel.

According to NIST (the National Institute of Standards and Technology), the biggest cyber risks infiltrating through supply chains come from the following:

1. Lower-tier suppliers with poor cybersecurity practices.
2. Compromised hardware or software used by suppliers.
3. Counterfeit hardware/software with embedded malware.
4. Software vulnerabilities in supply chain management systems.

For more cyber supply chain risk management best practices from NIST, visit **https://bit.ly/2PVpe5s**

While you cannot always enforce security standards on your partners, being aware of potential risks and choosing your partners wisely can go a long way toward maintaining a secure supply chain. Ask them the same cybersecurity questions that you will be asking yourself as you go through this guide. Make sure that they have robust IT security policies internally and processes for ensuring the safety of your data. Look for risk management benchmarks such as industry or government cybersecurity certifications.

part two

Best Practices

A good first step toward improving cybersecurity for your business is to examine what is known as your cybersecurity "posture," meaning the current state of your business's cybersecurity.

This process typically starts with a thorough data audit. In addition to the advice presented in this guide, more information and free resources to assist you in your efforts can be found at cyberflorida.org/SMB.

The goal of this assessment is to build a comprehensive view of how your business compares to other businesses that have implemented cybersecurity best practices. A good assessment helps you determine where you are, where there is room for improvement, and how best to start plugging the gaps in your defenses.

Though a data audit can be challenging, you likely will become much more confident and stronger in your cybersecurity position for having gone through it. A good way to begin is by focusing on the core aspects that compose the foundation of protection for your business.

Audit Your Data

First things first: a data audit! Yes, nobody likes the word "audit," but take a deep breath and remember: it's you auditing yourself—no judgment, no cyber shaming here. You may not like what comes out of your audit, but what you absolutely must do is be honest with yourself about performing the audit so that you can make meaningful improvements. Nobody will ever know how bad things were before, unless you fail to fix them, and they become a problem later.

> In 2018, small businesses reported an average cost of $1.4 million in damage or theft of IT assets and infrastructure and **$1.5 million due to disruption of normal operations from cyberattacks.**
>
> Ponemon Institute

Data is everywhere these days, and it has the most annoying habit of slipping out of your grasp and into the open unless you are very careful with it. The problem with this is that it can cause significant reputation loss when discovered and may open the door to potential legal claims against your business. A data breach can effectively put you out of business.

Let's start asking some hard questions. What data are you collecting by design or by accident? Where do you store that collected data? How long do you store it for? How do you protect it? Write all the answers down, then go back to the question and remember the "by accident" part and think of anything you may have missed.

You simply cannot attempt to keep data safe until you can locate it and acknowledge that it exists and that it's probably not secure. That is why this step is challenging; you must ask yourself, honestly, "If this was my personal data, would I feel comfortable with the level of protection in place?" Often, the answer is no, and that's okay. The world of digitized data has grown rapidly in just a few years, and many businesses are struggling to keep pace. In a 2018 Ponemon Institute study, only 28% of SMB leaders rated their ability to mitigate cyber risks, vulnerabilities, and attacks as highly effective. What matters is that you are taking some steps toward improvement.

What Is Your Data?

Download the Data Audit Worksheet at cyberflorida.org/SMB to make a list of the data you know your company collects. Include the data you hold in your customer database system and accounts payable and receivable. Do you use point-of-sale (POS) machines to process credit cards? Lots of data for the list! You may have some website visitor tracking, social media analytics, or perhaps some email marketing. Add those to the list.

Got any old Excel spreadsheets with lots of customer details hidden away in a hard drive or filing cabinet somewhere? Add that to the list as well. Company payroll and HR files? Very sensitive data for the list. Finally, let's not forget about the third parties who may hold your business data: suppliers, vendors, and contractors. If they have some of your customer data somewhere, add them to the list as well.

When you can't think of any other data sources, take a break, and then review the list.

Where Is Your Data?

Once you have a better idea of what your data is, this next bit is easy. You now should determine where that data lives, and once you figure that out, you can then turn to protecting that data.

For each bit of data you identified in the first question, note its physical and geographic location. Is it stored in the cloud or on an external hard drive at headquarters? Is it on a server at a regional office? Where is the backup stored?

You should now have a list of your data and know where it lives—you are winning this data audit!

Quick Wins for mobile devices.

KEEP A CLEAN MACHINE FOR ON-THE-GO DEVICES.

- Update security software regularly. Go ahead, update your mobile software now.
- Delete unneeded apps and update existing apps regularly
- Always download apps from a trusted source and check reviews prior to downloading
- Secure devices with passcodes or other strong authentication, such as fingerprint recognition
- Turn off Discovery Mode
- Activate "find device" and "remote wipe"
- Configure app permissions immediately after downloading
- Learn More: ***https://bit.ly/2Qqhc02***

Talk to the Team

While you may be the boss, you may not be aware of everything your team does with your company's data. Be sure to talk to your team, and ask them about the data they handle so that you can add it your list. Talk to key staff members and leave no stone unturned. Employee data handling practices are a blind spot for many businesses. Leaders often think they know their company's data flow, but employees often create their own workflow and may be handling data in ways you don't realize. Including your employees in this process also lets everyone know that you take your business data seriously, which helps create a culture of cyber awareness.

Rank Your Data in Terms of Value

It's important to know which of your data is the most valuable so that you can prioritize your investment of resources. High-value data is both data that may be an attractive target for cybercriminals, such as credit card information, as well as data that is critical to your business functions.

For example, if you are a mail order delivery business, then your customers' address details will be high-value data—your business cannot function without it. Perhaps you own a walk-in store that does not actively gather customer data? In that case, your vendor data and your POS data—created when processing customer credit card transactions—are the most valuable data in your business. Low-value data is data that does not contain personally identifiable information (PII), such as names along with social security numbers, birthdays, and addresses—information that is tied to a specific person. Things like office policies and marketing collateral, which, if it fell into the wrong hands would cause no damage to your business or customers, are low-value data.

Rank all your data in terms of value to your business. Once you know exactly what your high-value data is and where it lives, your data audit is nearly complete. When it's all over, you likely will feel much more confident when it comes to thinking about data and its value—a huge first step on the road to cybersecurity!

Determine How You Currently Protect Data

Now that you have a more accurate understanding of what data you have, where it lives, and how valuable it is, it's time to determine what kind of safeguards you have in place to stop that data from leaking. First, review the Data Protection Best Practices section to familiarize yourself with some basic cybersecurity safeguards, then examine how you are protecting your data. Which of those safeguards do you currently have in place? Who has access to databases? Are databases encrypted when not in use? Assess whether your website uses a secure HTTPS connection, if you need to limit access to certain parts of your website, and if there is any data on your web server that should not be there.

This is also the time to think about passwords. How strong are the passwords used to secure your data? How often are passwords reused across the business, and how frequently are passwords changed? Ask your third-party vendors and suppliers about how they secure your data and demand they take your valuable data as seriously as you do.

Now that you have a better idea of what data you have, where it lives, who uses it, who has access to it, and how it is secured, you are well on your way to properly assessing the cybersecurity risks in your business. The next step is to consider the threats unique to your business.

Threat Modeling

Threat modeling is the process of figuring out who your potential cyberattackers are likely to be and which data they would be after if they decide to attack you. You must try to think like an attacker. Going through the threat modeling process will help you identify some of the security doors that you may have left open and if you left any of your high-value data in an accessible place. Ideally, you want to get a glimpse into your potential attacker's mind, motivation, and thinking.

Ultimately, "threat modeling" is a fancy name for something that you do every day. For example, if you were asked to threat model the warehouse of an electronics retailer, you would probably say something like, "Criminals will definitely try to rob you because you store boxes of expensive electronics in your warehouse. You need to get some bars over the windows and locks on the doors. You should also install an alarm system and maybe get a guard dog or two." That, in a nutshell, is threat modeling.

Create a threat model for your business. The goal is to reduce your attack surface, meaning the number of potential entry points that an attacker can use to enter your business. An entry point could be a shared password, client data on an unsecured server, an operating system that has not been properly updated, or the lack of password protection on your database. It is impossible to know if you've found every potential vulnerability, but this process should help reduce your potential vulnerabilities.

Threat Modeling

To craft a threat model for your business, answer these important questions:

What Is It That We Do?

Through the eyes of an attacker, meaning if a criminal looked at your business, what is it that you do that s/he would find of interest? The answer will likely overlap with what you have identified as high-value data for your business, but occasionally you may find differences. **For example, did you know that airline miles and travel reward points are hot items for sale on the dark web?** That information may not be critical to your business, but it is a high-value target to a cybercriminal. Criminals also look for social media accounts to conduct reconnaissance for other crimes. So, once again, consider all the data you collect, but this time, try to think like a criminal. Maybe you collect obvious target data, such as customer financial records, medical records, or financial transaction data. Perhaps you use point-of-sale devices or maintain a customer list. Consider intellectual property as well. **Is it the web app you developed or the widget you designed and built?** Look at processes. **Does your accountant send money if you instruct them to by email, without calling to check that it is a valid request from you?**

What do you do that they would find interesting? What would they steal? Answer these questions, and you generally will have a much stronger idea of what you should be protecting.

Where Could A Cybercriminal Infiltrate?

What are the known points of access, and who uses them? Could it be with that password you have always used and share with contractors? It might be that you use the same password across multiple accounts or that a contractor who ceased to work for you three months ago still has access to your CRM system. Do any of your software or equipment vendors maintain points of entry to their products? Don't forget to consider physical access points as well. Many breaches have resulted from stolen laptops.

Try to imagine how you would attack your own business if you were a criminal. Where would you start first? Where do you think that your own security is the weakest, and how could you get the credentials you need to gain entry? The goal is to identify what could potentially go wrong in your business—potential backdoors and weaknesses that a cybercriminal could exploit.

This is a good time to dive deeper into something introduced in the first section: social engineering. Remember that it's easier to hack people than it is to hack systems. When you're considering points of vulnerability in your business, employees should be No. 1 on your list.

Social engineering is the most common tool used to hack people. Instead of spending a lot of time probing your IT systems for vulnerabilities, it is far easier for a criminal to call one of your people and pretend to be one of your employees. We often hear about hackers pretending to be IT support technicians and tricking employees into giving them their passwords. This is a very real threat and another reason to invest in training your employees.

What Are We Going to Do About It?

Review the data value categories you created earlier and your answers to the last question. What can you do to reduce or eliminate the potential vulnerabilities you identified? Do you really need a shared team database password? Sure, it's convenient, but perhaps everyone should have their own password so you can tell who has been logging into the system?

Maybe it's time to encrypt the data that you have sitting on your server, or perhaps it's time to update your workstations and implement a periodic upgrade schedule. It could be that your passwords need changing and that you need to adopt the use of password managers in your business. Refer to the Quick Wins listed throughout this guide, as well as the Data Protection Best Practices section, for guidance on some actionable steps that you can choose to implement right now to likely improve your cybersecurity posture.

How Did We Do?

This is the point where you take a long, hard look at everything that you have learned so far, every problem you've discovered, the actions that you've taken to mitigate them, and finally, appraise your efforts as best as you can. By working through this threat modeling process, you likely will begin to understand how an attacker might look at your business, and you can use that improved understanding to develop and hone your cybersecurity awareness and practices over time.

How Much Security Is Enough?

This is a difficult question to answer for any business. Industry standards will be reviewed in the "Good, Better, Best" section, but ultimately, it comes down to each business to determine what an adequate level of security is given the financial resources available. The actions you listed above to reduce your security risks to an acceptable level are totally dependent on the value of the property or data at risk, as well as the consequences if the worst-case scenario were to happen and you were attacked.

For example, if you manage a fruit and vegetable stand, and hackers break into your computer and steal your supplier list, that attack would probably not have a devastating impact on your business. You could get away with having minimal security. But if you own a bakery with a secret 300-year-old recipe that you use to make your flagship product and that is stolen in a cyberattack, then it could potentially have a devastating impact on your business as your competitors can now make the same treat and undercut you. In this case you should consider doing everything possible to defend your intellectual property.

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

1. What is the value of what you need to protect? This can be a product, service, data, a process, your invention, financial transactions, or even professional relationships (value can express itself in many different ways).
2. To sustain the value of your business, what needs protecting? This can include information, technology (either hardware, software, or systems), your facilities, and your employees. It is likely that a blend of these is what gives your business value.
3. What could happen if it's not protected? An unfortunately large number of small businesses who experience a cyberattack do not recover from them and go bankrupt within a short space of time. While a large business might have cyber insurance in place and the capital to absorb the financial and reputation loss that a cyberattack can bring, many small businesses do not. While it's scary to think about, you should ask, "What would happen to my business?"

What is on the Dark Web Menu?

Credit card data	$7–$100
Banking and online payment credentials	$100–$1,000 *depending on account balance*
Airline miles	50,000 for $98.88
Social media login credentials	1,000 for $25
Forged Prescriptions Large U.S. Drug Stores	$50–$100
Hacking Tutorials	$5–$50 *Multiple Tutorials*

Armor, *The Black Market Report: A Look Inside the Dark Web*

Today's Special

U.S. Green Cards
Driver's License
Insurance
Passport Visas
(bundled)

only $2,000

Employee Training

It is almost a cliché in the cybersecurity world: if you ask 100 cybersecurity experts how they would spend $1 million to improve an organization's cyber resilience, 99 of them would say, "Employee training."

It is much easier for a cybercriminal to exploit human nature than to penetrate a firewall. This statistic bears repeating: 93% of data breaches began with a phishing attack (*2018 Verizon Data Breach Investigations Report*). Your employees are your first line of defense against cyberattacks, and employee cybersecurity training is essential to improving your cybersecurity posture. If your people are trained on the risks and become cyber aware, they can very often prevent an attack.

Many cybersecurity experts think that employee training is the weakest link in a business's cybersecurity strategy, primarily because many businesses neglect to spend money on employee training, even as they spend money on other cybersecurity measures. Employee training can even reduce cyber insurance premiums. Leaving employees out of the process is short-sighted and puts your business at risk.

a case study

If your SMB implements only one tip from this guide... **train your employees!**

Don't Blame the Victim

A cybersecurity professional was speaking recently with the senior leadership team of a large retailer. One executive revealed that their recent cyberattack was caused by one employee who clicked on a malicious email attachment that installed malware onto his computer. That malware then made its way through the organization's networks. The executive stated that they saw the employee as the weakest link and placed the blame on that individual. The cyber professional pointed out that the employee had done nothing wrong and that, because they had failed to train their employee in even basic cybersecurity awareness, the fault lay entirely on their doorstep. How can the employee protect against a cyber threat that they do not understand or expect? They cannot.

If that employee had passed through cybersecurity awareness training, he might not have clicked on that malicious attachment. Instead, he might have double checked that the sender email belonged to a legitimate business contact and thought twice about why that contact was sending him an attachment.

Employee awareness training is one of the most cost-effective investments you can make in your business's cybersecurity. No amount of physical or technological protection will save you if your employees mistakenly hand over their login credentials. At a minimum, ensure that your employees receive a crash course in cybersecurity basics at least once a year. Ideally, provide ongoing, comprehensive training that makes cybersecurity a priority across your business. It can make all the difference if your business comes under attack.

Visit cyberflorida.org/SMB for a list of free employee training resources.

advice from the experts

Dr. Ronald Sanders
Cyber Florida Board Member, Director and Clinical Professor,
University of South Florida School of Public Affairs

Cybersecurity: It's All About the Culture...

Introduction: It's the 'Wetware' that Really Matters

These days, organizations both private and public are faced with a daunting variety of threats to their cybersecurity, not just from criminals and hacktivists who are out to steal and sell (or reveal) personally identifiable—or organizationally embarrassing—information, but also from state and non-state actors who are after priceless intellectual property, some of it classified Top Secret. And while those threats are increasing in sophistication and persistence, many of the most notorious cyber breaches are the result of nothing more than poor 'cyber hygiene'—that is, an insider who unwittingly responds to a spearphishing attack, reveals a confidential passphrase, or plugs an infected device into the network.

Regardless of the attack vector, it is clear that cyber threats can be existential in nature—not only can those threats impact the livelihoods of all those who trust a particular organization to safeguard the information they give it, whatever it is, but they can also threaten the very existence of an organization as well as the jobs of its C-suite officers. Whether those officers are legally liable for a network intrusion, or whether they are just administratively or politically accountable, the fact is that cybersecurity (or lack thereof!) can put customers and citizens, vendors and shareholders, and executives and organizations all at risk.

Thus, the stakes are high, and at first blush, protection of an organization's data and networks seems like a technical challenge of the highest order. So as long as an organization's senior leaders pick the right Chief Information Officer or Chief Information Security Officer, and give him or her the resources and talent that they need, their job is done, right? I would argue that this is not only wrong, but risky in the extreme. Sure, the technical side of cybersecurity is critical, but the statistics show that it's an organization's culture that may matter most.

advice from the experts

Cybersecurity: It's All About the Culture...

As Mike Rogers, former Director of the National Security Agency and U.S. Cyber Command, used to say, it's the 'wetware'—the people—that really matter. The most obvious aspect of this has to do with cybersecurity talent—the cyber ninjas that serve as an organization's front-line defense against intrusion. There can be no doubt as to how vital that talent is, nor is there any doubt as to how hard it is to get and keep. There is a growing gap between the demand and supply of such talent, one that requires national attention, but that is for another time (and another paper). I'd like to focus on a less obvious but no less vital aspect of an organization's wetware: its culture.

> Sure, the technical side of cybersecurity is critical, but the statistics show that it's **an organization's culture that may matter most**.

Why is culture so important to one's cybersecurity? Just look at the statistics. Historically, 80% or more of cyber intrusions stem from human error, most often an employee inadvertently opening an email that they shouldn't, revealing a password where they shouldn't, or copying and leaving files somewhere where they shouldn't. And these are all inadvertent and unintended. When you add malicious insider intent—from a disgruntled employee, for example—the percentage climbs even higher. And these are all examples of behaviors that are influenced by an organization's culture. And I would argue that that's the exclusive responsibility of the organization's senior leadership team. It doesn't matter whether the

advice
from the
experts

Cybersecurity:
It's All About
the Culture...

organization is in the private, public, or non-profit sector. An organization's cyber defense is not just about the skill (and trustworthiness) of its IT and cyber talent, but also about the efficacy of the organization's culture. Both are crucial to preventing, detecting, and responding to an attack.

A Cyber-Secure Culture Defined

What does that culture look like? As a practical matter, it is a collection of symbols and rituals, beliefs and practices, and other organizational artifacts—some deliberately and formally established, but most often not—that have a profound influence on how an organization's members behave. Think of culture as an organization's collective 'mindset' (as opposed to its skill set), with employees typically taking their cues in that regard from a variety of sources, to include lofty pronouncements of policy from the C-suite, but also their immediate co-workers and supervisors. In other words, culture determines 'how we *really* do things around here' and manifests itself in individual behaviors that become second nature.

Translate that to an organization's cybersecurity mindset, especially among those of its employees—for example, in sales and marketing, customer service, or production—who are far removed from the daily cyber-skirmishes that take place in the Network Operations Center, but who depend on the outcome of those skirmishes to do their jobs. Those employees are not innocent bystanders either. If they have access to an organization's data and networks, they are part of its vulnerable 'attack surface' and as such, can also have as much an impact, witting or unwitting, on an organization's cybersecurity as its front-line cyber troops. Are they lax or vigilant when it comes to spearphishing attacks or the security of passwords? If they "see something (such as anomalous network activity), do they say something" to someone? Do they report suspicious behavior on the part of a co-worker as a possible a signal of a cybercrime in the making?

Obviously, these employee behaviors—that is, their work habits, both good and bad—are profoundly influenced by the organization's culture. And if one of those habits happens to be opening an unfamiliar email without thinking, that can put the entire organization at risk. That scenario is all too familiar—just ask all those organizations that have been victimized by a spearphishing attack. Upwards of 80% of all successful breaches can be traced to poor cyber 'hygiene,' that is, workplace behaviors that literally leave the cyber back door open.

It's a Mindset, not Just a Skillset

The above are all examples of a cybersecurity culture that is decidedly *un*secure. But for those that are tempted to throw up their hands and lament that it is just human nature, the good news is that these are all behaviors that are correctable. I don't want to minimize an organization's challenge in that regard, but all it takes is good 'cyber hygiene' to mitigate, if not avoid, many of the risks associated with human nature, especially when it involves work-related habits that can be shaped by culture.

More importantly, that culture need not—indeed, cannot—be left to chance. We know (from research as well as experience) that culture can be deliberately shaped. But it takes more than just a policy pronouncement in your organization's new employee orientation, or mandatory annual online training, to make it part of your organization's mindset. Like other core work-related values—for example, ethical behavior, customer treatment, employee engagement, diversity and inclusion—good cyber hygiene must become part of an organization's collective psyche. The good news is that mindset can be diagnosed, and where it is found to be problematic, it can be retooled. For example:

Recognizing and Reporting. Do employees know how to recognize potential cybersecurity risks—not just spearphishing attacks, but physical and other, more subtle information security risks, including their own and/or a co-worker's behavior? Training and education are key here, not just in formal settings (like a classroom or orientation session), but constantly on the job, from informal coaching to simulated spearphishing attacks or cyber hygiene 'pop quizzes' that control system access. And it isn't just employee training. Cyber situational awareness and vigilance is also part of a cyber-secure culture, and managers and executives all need to understand their non-technical role in shaping it, especially when it comes to recognizing, reporting, and responding to potential cyber risks. For example, if employees see something, will they say something, even if it puts them or a co-worker in jeopardy? In many respects, culture is an organization's collective conscience, and that conscience can be shaped to encourage these workplace behaviors, or they can be left to chance.

Reinforcing and Rewarding. What has happened to employees who have reported potential cybersecurity risks (or violations) in the past? Is there a program to acknowledge, recognize, and even reward those who report cybersecurity risks? Are managers at least encouraged to offer informal recognition and reinforcement? Or are cyber whistleblowers ignored, ostracized, or even punished (formally or otherwise)? Formal amnesty and 'hold harmless' policies help, as do anonymous tip-lines or even ombudspersons. All of these come with their own risks, but employees will look to what actually happens to other 'whistleblowers' (cyber and otherwise) when they contemplate joining their ranks, so this can be critical. Some organizations even go so far as to make cyber hygiene a part of an employee's annual performance evaluation, but this can only work if the organization's culture is aligned with that requirement. If poor or lax cyber hygiene is informally tolerated, formal evaluations are meaningless.

Some organizations even go so far as to make **cyber hygiene a part of an employee's annual performance evaluation**, but this can only work if the organization's culture is aligned with that requirement...

Morale and Moral Suasion. It's also plausible to assume that cyber risks—especially the human kind—are a function of employee morale and engagement, and these too, are a product of an organization's culture. The relationship may be indirect—I know of no research that makes that connection empirically—but it makes intuitive sense that employees who are engaged and motivated are more likely to pay attention to, avoid, or report cyber risks that may threaten the very existence of their organization. Morale matters to an organization for so many things, and cybersecurity is one of them. Our nation's intelligence agencies know this; they regularly administer climate and other employee surveys to their workforces, not to ferret out individual bad actors so much as to determine if their agency's culture and climate are conducive to them. Exit surveys are another source of information in this regard. Simply put, unhappy employees are cyber risks, and the organization needs to establish some sort of early warning system to identify and mitigate the risk.

But make no mistake: there's a darker side to cybersecurity that cannot be shaped by an organization's culture. No matter how 'cyber-secure' that culture may be, there will always be the risk of malicious insider threat, someone with nefarious intent who wittingly seeks to compromise an organization's data or networks. For most organizations, the greatest of those insider threats is 'home grown' in nature—that is, from an otherwise-trusted and loyal employee who had a spotless record—until something happens at work. It could be an impending layoff or an unsuccessful bid for promotion. Or it could even be off-duty

advice from the experts

Cybersecurity: It's All About the Culture...

in nature, ranging from extreme indebtedness to substance abuse and addiction. There is always that risk, that a disgruntled or disaffected employee, especially one that is part of an organization's attack surface, may decide to try to profit from his or her access, or even 'take it out' on his or her employer. Surveys can't anticipate that kind of threat (there are other ways to do that), but those leaders that have their fingers on the 'pulse' of their organization—that is, how employees feel about working there—and act on what they learn can at least serve to minimize them.

A C-Suite Responsibility

So, in my view, it all comes down to an organization's culture—the collective mindset that can have such a profound influence on the behavior of its 'wetware.' And as noted, that culture is not an immutable feature of an organization's environment, something beyond its control. Rather, it is a social phenomenon that can be deliberately shaped to align and support an organization's strategic goals and core values—including cybersecurity—and that's squarely in the C-suite's job description.

There's ample proof that culture can be shaped, and I've tried to offer just a few of the techniques that other organizations have employed to do so. This is not an academic paper, so I'll spare readers a long list of references, but one of those is especially worth reading: Dr. Edgar Schein's seminal work, *Organizational Culture and Leadership* (fifth edition, with Peter Schein; published by Wiley in 2016); it describes many of the strategies that leaders can employ to shape culture, and it's no stretch to apply them to cybersecurity. So, suffice it to say that there's plenty of empirical research—not to mention lots of practical experience—that tells us that an organization's culture is there to be molded, and that it's the organization's leaders that are responsible for doing the molding.

To be sure, the organization's CIO, Chief Technology Officer, and/or Chief Information Security Officer all share some of that responsibility, at least from a technical standpoint. After all, it's their job to minimize the attack surface available to a potential cyber thief, whether they're inside or outside the firewall. But there will always be an attack surface, and at the end of the day, good cyber hygiene comes down to ensuring that individual employees understand, internalize, and behave according to a common set of cybersecurity standards—just as we would expect them to comply with standards of conduct, ethics, non-discrimination, and the like.

Bottom line: The benefits of a strong culture to an organization—especially one that addresses cybersecurity—are innumerable. Obviously, as a general matter, a culture that engages and motivates employees can help an organization recruit and retain talent; cyber talent is no different, and given today's hypercompetitive cybersecurity job market, that can be critical. However, there's so much more to it. Given its impact on employee morale, a strong and supportive workplace culture can minimize the odds of a 'lone wolf' insider with malicious intentions. And if that culture also emphasizes and encourages (and even incentivizes) cyber awareness and hygiene, it can also help every employee be as vigilant as an organization's Network Operations Center when it comes to seeing and saying something, whether it's unwitting or inadvertent lapses—the single most prevalent cause of breaches and spills—or suspicious behavior that may signal a bad actor on the prowl.

Surely that's worth the time and attention of an organization's senior leadership.

Protecting Your Data

Good, Better, Best

The good, better, and best guideline can help you consider how much security you should have in place. When used in conjunction with your data audit and threat model, this system provides a rough measure of how much security you should consider to better align with industry standards across the nation.

Good (Defend) - Good security is considered basic defensive security, like having a firewall to keep unauthorized intruders off your network, enforcing the use of a password manager, making sure all your software and operating systems are regularly updated, and providing basic cyber awareness training for your employees. The Quick Wins listed throughout this guide and the action items listed in the Data Protection Best Practices section will help guide you toward good security practices.

Better (Monitor) - Better security is when you are actively monitoring every aspect of your IT infrastructure, looking for strange traffic patterns, network anomalies, and malware activity. This is usually automated and managed by technology solutions or third-party vendors that alert you of suspicious activity.

Best (Prevent) - A preventative level of security is considered best; it can range from penetration testing (paying an ethical hacker to attempt to infiltrate your systems and tell you what to fix), investing in customized employee cyber awareness training, testing your IT infrastructure and software, or even monitoring the dark web (the underground criminal web) for any mention of you and your employees, data, or customers.

So, for example, if you manage an ice cream shop, you want to have good security in place to protect your Wi-Fi network, router, and POS system from attack. If you want to protect a money lending business, you should have better security in place to protect customers' financial information and transactions. If you are an engineer working on a new medical device, you should have the best security in place and actively work to prevent your intellectual property from being stolen.

The NIST Cybersecurity Framework

NIST, the National Institute of Standards and Technology, is an agency of the U.S. Department of Commerce tasked with promoting innovation and industrial competitiveness. NIST fulfills this mission by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST is highly regarded throughout the industry for setting the standards around IT security. The NIST Cybersecurity Framework, formally titled "Framework for Improving Critical Infrastructure Cybersecurity," provides guidelines and standards that are applicable to any organization. In NIST's words, the Cybersecurity Framework "consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."

While it is not a one-size-fits-all solution to cybersecurity, the framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders and identifies the common challenges, processes, and practices that define cybersecurity. The guidance offered here aligns with the standards and practices prescribed by the NIST Cybersecurity Framework. You can learn more and access a wealth of free resources online at **https://www.nist.gov/cyberframework**.

The crux of the NIST Cybersecurity Framework centers on these five functions: identify, protect, detect, respond, recover. These are the five core functions every business should engage in to achieve what is widely considered an adequate cybersecurity posture. So far, you have addressed **"identify"** by conducting your data audit and **"protect"** by building your threat model and evaluating your current security practices. Now, consider elevating your cybersecurity from good to better through detection.

Time to Bring in the Pros?

No matter how well you perform your audit and threat modeling, at some point you may want to consider bringing in a professional.

If your business cannot afford to hire a security manager or bring in an external cybersecurity consultant to validate your efforts, then try to find a good IT person who can come in for a day, take a look over everything that you have done, and make recommendations. Good IT systems administrators are much less expensive than cybersecurity experts, and they typically understand the fundamentals of IT security and can offer you guidance for a reasonable fee.

Another option is to explore if any colleges in your area offer cybersecurity programs. Instructors are often looking for opportunities to engage students in real-world practice, and evaluating a small business's cybersecurity makes a great class project. Similarly, cybersecurity graduate students can be a great source of low-cost expertise.

At the very least, seek out an experienced IT systems administrator to go over your data audit, threat modeling and good, better, best calculations. S/he may be able to spot things you may have missed and make technical recommendations.

If you have some money to spend on cybersecurity, you likely may be thinking about either hiring your own security person or bringing in a vendor to help you. But how to choose?

Many businesses hire employees who are central to the core operational purposes of the business and outsource tasks to freelancers or consultants who are not central to core business activities. If a task is not big enough to justify the expense of a full-time role, typically those tasks are outsourced, too. But what about your cybersecurity? Should you hire an employee or bring in the consultants?

There are pros and cons to each. When you hire consultants, you save the overhead of paying for an employee, but you also give up a degree of control over your security processes and practices, as the consultants call the shots. Hiring a consultant means that you give a third-party access to your security and systems, so it's best to make sure that you trust them. Using consultants may be a significant cost; however, they typically have a lot of experience and resources and are actively "plugged in" to the current threat landscape. They may find infiltration points and potential threats that an internal security team would not. Additionally, many cybersecurity firms are aware of the struggles small businesses face and offer free services and reduced rates to SMBs.

When you hire an employee, you get a core member of your team managing your security, one who is more likely to be loyal to your business first. That person is dedicated to nothing but ensuring that the value in your business is kept safe from a cybersecurity perspective. However, such expertise can come at a very high cost. If you would like to move your business toward "better" or "best," then a full-time cybersecurity employee is worth exploring.

What Questions Should You Ask?

The market is full of cybersecurity experts, thought leaders, evangelists, and freelancers who sound like they speak a foreign language to the average business owner. If you are not used to being around technically minded people, it can be quite intimidating to speak to them, especially when you don't understand them.

Ask them to use analogies - Their ability to clearly articulate a complex technological idea in a way you can understand is essential to your future relationship with this company. They should to be able to explain security risks and processes to you in plain English, and analogies are the best way to do this. A good cybersecurity practitioner will be good at using analogies. Remember what Albert Einstein once said, "If you cannot explain something simply then you do not understand it well enough." So if you find yourself feeling lost or overwhelmed during the conversation, try someone else.

Quick Wins for Wi-Fi security.

THINK BEFORE YOU CONNECT.

- Use separate Wi-Fi for guests or customers than you do for business
- Physically secure Wi-Fi equipment
- Use a virtual private network (VPN) when using public Wi-Fi
- Do not connect to unknown, generic, or suspicious Wi-Fi networks. Use your mobile carrier's data plan to connect instead.
- Turn off Wi-Fi and Bluetooth when not in use on your devices
- Secure your internet connection by using a firewall, encrypt information, and hide your Wi-Fi network
- Learn More: ***https://bit.ly/1Dlhprx***

Ask them about your core security risks - A good cybersecurity practitioner should be able to identify where some of the core security risks in your business are and talk about them, before basing their security recommendations on those core risks. Unless the consultant or employee can identify these risks, it is unlikely that they will be able to properly advise you on how best to invest in your security.

Ask them who will perform the work - Many consultancies will send one of their senior practitioners to come and talk to you, convince you that you are in good hands. But when it comes to performing the work, they may send in a junior employee or beginner who is fresh out of college and probably training on the job as s/he goes, completely lacking in professional experience. Make sure you know who will be performing the day-to-day work. A junior employee or beginner may not be a problem, so long as they have good supervision.

Ask them about their mistakes - Good consultants can adequately evaluate your security risks and penetration test your networks without bringing your networks or IT infrastructure down for unscheduled maintenance. You do not want to know about the times the consultant did a great job; you want to know about the times they failed and why. Even the best cybersecurity operators make mistakes from time to time, and the best of them openly and freely admit it; the bad ones don't. They should be willing to share a failure with you, as well as what they learned from the experience.

Ask them about their certified and practical experience - Be wary of fancy certificates. Many legendary cybersecurity people and many of the people on the front lines have no certificates but are quite knowledgeable. Then there are those with lots of certificates but no real practical experience. In cybersecurity, hands-on-keyboard experience is more valuable. Ask them about their practical experience.

Ask them if they will train your employees - This one is so important, and it is essential that the consultant answer this question correctly with a resounding, "YES!" Many consultants think that employee training is beneath them; those who feel that way are doing your business a disservice by overlooking one of the most critical parts of cybersecurity. A reputable consultant should believe that it is their job to teach people how to defend themselves, not just come in and fix your security gaps. Remember that your employees are prime targets for hackers; they likely would rather send a few phishing emails to your team than spend hours looking for a technological vulnerability. Employee training is a valuable and cost-effective measure, and It should be a standard part of your consultant's services.

Cyber Resilience

in their words

> "User confidence is crucial for digital economy. Customer as a product and unsafe privacy are not sustainable business models. Digital is sophisticated enough to combine security, convenience and personal privacy."
>
> *–Stéphane Nappo*
>
> *Global Chief Information Security Officer*
> *at Société Générale International Banking*

Now, we move on from **"detect"** to **"respond"** and **"recover,"** which can be summed up in one word: resilience. Resilience reflects your ability to bounce back from a business disaster, in this case a cybersecurity disaster, and it has become a critical component of cybersecurity. Because cyberattacks have become so widespread, many experts advocate that everyone should have response and recovery plans in place, not if they are attacked, but when. Making your business more cyber resilient means you will be better prepared to weather a cyberattack with minimal disruption and data loss.

Imagine the worst-case scenario: say your business came under a ransomware attack from a 15-year-old hacker calling himself Pharaoh Snefru—bravado is a hallmark of young hackers.

Young Snefru has recently discovered the wonderful world of ransomware-as-a-service—inexpensive tools and services for sale (or rent!) on the dark web that make it easier for inexperienced hackers to cause you a lot of trouble.

Pharaoh Snefru does some basic reconnaissance and discovers that your customer service manager, John, has his email address posted on your website and that John likes to exchange messages on social media with a winsome woman named Jane. Young Snefru quickly sets up an email account using Jane's name and emails his ransomware package to John, who feels butterflies in his tummy when he sees it.

An email from Jane! And she sent me pictures! Click.

Suddenly you have a cyber disaster on your hands because John has unwittingly clicked on a phishing email from Snefru that contains an aggressive strain of ransomware. That click you heard John make on what he thought were pictures of Jane was actually the sound of all of your business data being encrypted.

Now Pharaoh Snefru is in charge and even worse, his demands are outrageous.

You see, Snefru is not an experienced hacker. He is young and inexperienced, and he does not know enough to look at your business objectively and roughly determine a ransom appropriate for your resources. He asks you for one million dollars.

Even worse, he is on social media boasting about his "achievement" while your business seizes up from lack of access to the data that you need to function.

Snefru is drunk on his own success. By now he has told all his friends about his exploits, and they are egging him on and abusing you on social media, too. You tried to talk to him, but all you got was a GIF of a laughing Sphinx with the words, "one million dollars," emblazoned in all caps.

Your customers are noticing, and they start using all caps, too.

That is just about the worst cyber disaster that one can imagine for a small business, and it really happened. Cybercrime investigators report that many cyberattacks are perpetrated by children and teenagers like Snefru. Professional cybercriminals typically will unlock your data after you pay them a small ransom because the success of the next attack depends on a profitable resolution to the current attack. If you get a reputation for not unlocking data upon payment, your victims will stop paying. But youthful offenders aren't thinking logically.

If you want to be able to tell Snefru and his ilk to take a hike, you need a cyber-resilient business, and that means crafting a Business Continuity and Disaster Recovery Plan. Business continuity planning is the foundation of good cyber resilience and can help keep your business functioning during a cyber disaster.

Here the focus is on the **"recover"** aspect of the NIST framework (**"respond"** is the focus of the next section). When your business is disrupted, it can cost real money. If you lose any revenue and your costs increase, it may have a severe impact on your profits, and insurance companies may not fully cover losses or help you win back the customers you lost. You should have a well-thought-out Business Continuity and Disaster Recovery Plan in place.

First, create a business continuity plan. This is your business's strategy for recovering and maintaining operations in the event of a disaster. There are four basic steps to creating a business continuity plan:

1. Determine which part of your business operations are mission critical or time sensitive, and identify the resources (technology and people) that support those areas.
2. Determine how you would recover these operations in the event of a cybersecurity incident. What resources and preplanning are needed now to keep operations running smoothly when an incident occurs and to restore any lost data in the aftermath.
3. Assemble a business continuity and disaster recovery team from your employees, and collectively sit down and write a comprehensive plan with clearly assigned processes and responsibilities.
4. Train, train, train your people and conduct mock disaster exercises to make sure that your plan and your people know what to do. Many businesses get as far as Step 3 but stop short of Step 4. Your plan is not complete and in place until it has been tested and you know you can count on it when the time comes.

Determine Which Business Operations Are Critical: In the industry, this step is called a Business Continuity Impact Analysis, and the name almost explains itself. An impact analysis should properly identify the impact that a potential disaster could have on your mission-critical operations. But first, you should determine what those critical areas are and document them. Once you have done that, you can likely use this information to make better decisions about recovery priorities.

Download the Business Impact Analysis Sheet at cyberflorida.org/SMB to help you with this. You should complete one of these for each department you have, which likely will allow you to see a more complete mission-critical picture from afar and properly prioritize the impact risks. Business processes and functions with the highest financial and operational impact are likely the ones that you will want restore first.

Determine How to Support Recovery Activities - Recovering business operations from a disruptive event requires time and resources. You should calculate how long it likely will take to restore mission-critical operations and exactly what resources you may need to do so. Download the Business Continuity Requirements Worksheet at cyberflorida.org/SMB to help with this. Each of your department managers should fill one of these out so that you have a more complete view of the resources and time you may need to recover your business. These resources could be people, technology, important records, utilities (electricity or internet), and also products and raw materials that you might need to get the job done. You should also consider building in redundancy for each of these areas on that chance that one or more of them is affected by the disaster.

Assemble Your Continuity Team - Consider them your A-team for when disaster strikes. These are the people who know what the restoration priorities are and who know what to do when the worst happens. This step should be done in collaboration with your team, writing your business continuity plan as you go. Your plan should detail the aspects of your business that are vitally important, those which need to continue operating, and exactly how much time you have to restore those functions should disaster ever strike.

In short, you should plan your recovery strategies. If your business is hacked or your data is encrypted by ransomware, you should have a plan that will tell your continuity team exactly what to do when the worst goes wrong. This could be anything from relocating your key staff or contracting a third party to take over a vital function.

Training, Testing, and Exercises - Now that you have your impact analysis and your disaster recovery strategies planned, it is a good idea to test those strategies to make sure that they likely will work as expected. Conduct mock disaster exercises and train your people so they know what to do, and where to find answers in case they forget. Many experts advise running these exercises at least once a year, and while you are doing so, validating your recovery strategies so that you know they are still sound.

Having a viable Business Continuity and Disaster Recovery Plan in place as well as backups for your critical data are two essential components to help your business quickly respond to and recover from a cyberattack. Remember the words of Benjamin Franklin, "By failing to prepare, you are preparing to fail."

Quick Wins for social networks.

SOCIALIZE ONLINE WITH SECURITY IN MIND.

- Limit who has administrative access to your social media accounts
- Set up 2-factor authentication
- Configure your privacy settings to strengthen security, and limit the amount of data shared. At the very least, review these settings annually.
- Avoid third-party applications that seem suspicious, and modify your settings to limit the amount of information the applications can access. Make sure you're accessing your social media accounts on a current, updated web browser.
- Learn More: ***https://bit.ly/1OL1RPF***

advice from the experts

Colonel (Ret.) John E. McLaughlin
President, IPR Consulting

advice from the experts

Is the Cloud Right for YOUR Small or Medium Business?

Is the Cloud Right for YOUR Small or Medium Business?

Utilizing the cloud for your IT needs can have benefits, but there are things you must be prepared for as you decide what services you want to use the cloud for. The cloud is much more than people realize; it can be a fundamental shift in your information technology and services, as well as how you provide services to your customers. It can provide great capacity, agility, speed, and flexibility, if it is right for you. This article will help you determine what benefits or detractions the cloud has to enable you to make an informed decision if your SMB can benefit from it.

There are a lot of benefits that can be derived from utilizing the cloud:

1. Cloud computing provides widespread access to your company's data from many locations. This can be from separate fixed facilities or mobile use. You no longer have to be concerned with latency or bandwidth concerns that you'd have if your data was all in your own on-premise data center. It's typically easier to access data in the cloud, and it is an excellent environment if your workforce or customers rely on mobile applications or data analytics.

2. Application centralization is another benefit. If your SMB relies on several key applications or databases, the cloud enables you to host them in one place instead of multiple locations. This will allow your IT staff to focus on other things since you no longer have to maintain care and feeding (patch, update, review logs, etc.) of the same applications in multiple locations. This may also cut down licensing costs and decrease the number or size of your data centers or IT workforce.

3. The cloud allows you to take advantage of the latest advancements in technology. You will no longer be stuck with either using the server you bought three years ago or having to decide to life cycle it early to upgrade your on-premise hardware. To be competitive, cloud providers often maintain newer technologies that you can select as a service.

4. The cloud can be an excellent test and development environment. Instead of having to purchase and maintain your own separate on-premises test or pre-production environment, you can spin one up rapidly in a cloud environment. This enables you to maintain these separate from your production environment so that you don't risk damaging the production environment with tests or experiments. It allows you to cheaply build a system and see if it works. If it doesn't, it is simple to tweak it or even spin up a completely new system to try.

5. Moving to the cloud can be a forcing function to update apps/databases/processes to modernize or streamline your company's operations or services. You may be able to retire some altogether. This may enable you to cut down on overhead, management, wasted time, or even improve customer service. Some providers or third-party support companies may be able to help with this.

6. There have been amazing improvements in capacity process, compute, storage, analytics, and more. The increased agility, speed, flexibility, and capacity could be game changers for your SMB. If you combine this with using some cloud providers packaged and simplified applications, code, and training materials it can enable average users to greatly expand their capability.

7. If your SMB can use them, Artificial Intelligence and Machine Learning (AI/ML) become a realistic capability for an SMB in the cloud, where high capacity can be provided as needed at a reasonable time and price. In conjunction with third-party providers, you may be able to use existing ML models, rather than having to write your own algorithms, which is generally impractical for an SMB on-premise due to the cost of hardware, software, system administrators, and data engineers that would be required.

The cloud may be able to benefit your SMB, but there are some things to plan or watch out for:

1. You need to understand what your SMB's technical and performance management requirements are in order to differentiate between providers, and select the best one for you. It is important to work with your provider to ensure exactly who is doing what, as a misunderstanding can be dangerous. Who is going to manage your apps and services in the cloud? It will probably still be you, so don't plan to lay off your whole IT department. Typically, there is a lot of shared responsibility operating in a cloud environment—figure it out beforehand and be prepared to pay for what you want them to do. Ensure you take system administration, management, and cybersecurity into account when you do your cost and Business Case Analysis (BCA). The initial quotes are far more appealing than a true Total Cost of Ownership (TCO).

2. You must thoroughly understand and plan how you are going to migrate your data to the cloud. If planned or executed poorly, migration to the cloud (or anywhere for that matter) can be catastrophic. Who is going to do the detailed planning and the execution? What data, applications, or services are being moved and which (if any) are staying on premise? Someone must command and control this operation. Don't take for granted that it will go smoothly without detailed planning, synchronization (some apps or data may need to move before others), and command and control. Test applications, databases, and processes to ensure they aren't broken by moving them into the cloud environment. Paying attention to this can enable a smooth transition for your SMB and not interrupt your business. Sloppy planning or execution can put your business offline and impact your revenues.

3. You must understand where your data will reside. Is it in a foreign country? Is your data now subject to foreign laws? Is it being properly backed up? If you choose to remove it from the cloud, who does that, how will it be done, and how much will it cost? Do they now own or have access to use your data? All are important questions to answer during your BCA and planning.

4. Who is doing what for cybersecurity, and does that cost extra? The answer to the second question is most likely, yes! Design it up front to include monitoring, analyzing, response, and other items. You can outsource this, but you must protect what is key to your company. Any hack can be embarrassing and can impact reputational business, but your customers' data may be critical to protect—both from reputational loss, legally (such as Europe's new GDRP laws), or direct revenue. Your data and Intellectual Property (IP) are key, too. It's bad if your data gets accessed, worse if it is stolen, but catastrophic if it's changed and can't be trusted! Ensure there are backups off-network that can't be hacked if the primary and on-network backup are hacked. Many vendors don't understand or take cybersecurity seriously enough. Security checks, code scanning, intrusion detection, anomaly detection, identity

advice
from the
experts

Is the
Cloud Right
for YOUR
Small or
Medium
Business?

advice from the experts

Is the Cloud Right for YOUR Small or Medium Business?

and access management, penetration testing, and other capabilities can be built into your service or provided by a third party, but you'll have to weigh the cost of paying for a level of security versus the cost of being hacked.

5. Do you have older and/or custom apps that may not be properly supported in the cloud? Migrating could also be your forcing function to get rid of those albatrosses!

6. Costing models. There are many different costing models; make sure you pick the one that is best for you. For example, you could pay for a function only when an event takes place, or scale up or down your environment as needed. Methods such as these save you from having to maintain a higher capacity all the time when you only need it episodically. It can save money when you want to use services such as machine learning, so you don't have to maintain the full-time significant computing power it requires. This should be an important part of your planning.

So, is the cloud right for your SMB? For many small businesses it's a no-brainer—use the cloud. It generally costs too much in hardware, software, licenses, HVAC, power, and IT staff to build and maintain an on-premise capability if you're a small business. Ensure you look at the key planning areas mentioned as you determine what provider, what services, who administers it, and what level of security you need. Medium businesses could go either way; it really depends on your business. Is it spread out? What is your IT requirement, etc.? Larger companies have frequently gone back to an on-premise environment after trying the cloud. The TCO may have turned out to be better for them on premise. But even the large businesses may want to use the cloud if they want to invest in AI/ML because those services are likely to be better in a cloud environment due to capacity and flexibility requirements for the analytics. You'll want to do a good BCA with a thorough TCO to decide. The total cost of ownership versus increased capability and modernization may be a tough decision, but it's yours to make.

Quick Wins for file sharing.

SHARING IS CARING, ONLY WHEN DONE SECURELY.

- Restrict the locations to which files containing sensitive information can be saved
- If possible, use application-level encryption to protect the information in your files
- Use file-naming conventions that don't disclose the types of information a file contains
- Monitor networks for sensitive information, either directly or by using a third-party service provider
- Learn More: ***https://bit.ly/2dwxFil***

part three

Crisis Management

John Chambers, former CEO of Cisco, famously said, “There are two types of companies: those that have been hacked, and those who don’t know they have been hacked.” These words are often quoted in the cybersecurity field as a reminder that our systems are so complex, with so many potential vulnerabilities, that even companies that employ best-of-the-best cybersecurity practices can still fall prey to a cyberattack.

Say, despite your best planning efforts, despite increased cybersecurity measures, and despite your whole team becoming more cyber aware and wary of common threats, your business has been hacked and data has been lost.

When crisis strikes, there is only one thing to do—manage it properly. When it comes to protecting the reputation of your business and your customer relationships, what matters isn’t so much that you’ve been breached, but what you do in the aftermath of that breach. Here some suggestions of what you should do in a cybersecurity crisis to help your business survive—the **“respond”** phase of the NIST Cybersecurity Framework—will be examined.

Rule Number One: Don’t Panic

When you discover that your business has fallen victim to a cyberattack, remind yourself not to panic. This is sometimes easier said than done, especially when everyone around you may be panicking, and some of your customers may be aware.

Reassure your staff that you have a Business Continuity and Disaster Recovery Plan in place and that your business has taken steps to prepare for this crisis event. Remind everyone that there are established best practices to follow when it comes to managing the fallout of a data breach, and you intend to do your best to implement them. Then, pull out your Crisis Management Plan (which will be reviewed shortly).

Rule Number Two: The Whole Truth & Nothing but the Truth

The whole truth and nothing but the truth may sound like something you would hear in a court of law, but you should start acting as if you were in a court of law and carefully consider the legal fallout of the crisis.

Immediately start engaging with the legal obligations that have just pounced upon your business before they engage with you. Your data breach means that your business is now subject to the statutes contained within the Florida Information Protection Act (FIPA) (or the applicable law in your state) and that you have some legal obligations to attend to. Again, don’t panic, if you get this part right, the force of the law can work in your favor and help you recover from the crisis.

FIPA requires that you report any data breach to affected consumers within 30 days of discovery. If the breach affects 500 people or more, you must notify the Florida Department of Legal Affairs as well. Read the full text of the act online at **https://bit.ly/2j5yt2f** to familiarize yourself with all obligations imposed by this law.

If the breach involves the personally identifiable information of more than 500 individuals, you should report it to the Florida Department of Legal Affairs, which can be a valuable ally in helping you investigate and remediate the breach.

The General Data Protection Regulation (GDPR)

If you conduct business in the European Union (EU) or have customers who are EU citizens, you likely are subject to the EU's General Data Protection Regulation (GDPR), and you should consider consulting a GDPR legal expert to help your business take the appropriate steps to comply with this regulation.

What is GDPR? GDPR came into effect across the EU on May 25, 2018, and is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR lays out the principles for data management and the rights of the individual, and it also imposes revenue-based fines that could, in theory, become eye-watering if the breach was big enough or involved clear negligence.

GDPR covers all companies—including U.S.-based organizations who may not think they are subject to GDPR—that deal with EU citizens' data, so it is a critical regulation for corporate compliance officers at many companies.

What Happens if You Fail to Comply? According to the EU's GDPR website, https://eugdpr.org, organizations that fail to comply could face fines of up to $22 million or four percent of their annual global turnover from the prior year, and EU regulators are very keen to enforce the GDPR regulations and financially penalize organizations who fail to comply.

What Are Your Reporting Obligations? Regarding data breaches, GDPR imposes an obligation on organizations to report certain types of personal data breach to their local supervisory authority. Your business must do this within 72 hours of becoming aware of the breach, and if your data breach involved the personal data of individuals and could potentially have an adverse effect on their rights and freedoms in some way, you have an obligation to notify the affected individuals without delay.

advice
from the
experts

Steve Berlin, Esq.
Litigation and Technology Law Associate,
Rumberger, Kirk & Caldwell

Florida's data breach notification statute carries significant civil penalties to covered entities that do not notify affected individuals, and if necessary, the State. The penalties are two-fold. First, the State may assess a fine of $1,000 per day for the violation for the first 30 days. After 30 days, the penalty increases to $50,000 a month with a cap of $500,000. Second, Florida's Department of Legal Affairs may bring a Deceptive and Unfair Trade Practice Act claim against the covered entity seeking injunctive relief and/or a judgment for actual damages.

The federal government also has separate penalties for certain sectors, such as financial regulation, healthcare entities, and defense contractors. In addition to these penalties, affected individuals may have increased civil damages as data breach victims.

Does GDPR Impose Any Other Obligations? GDPR specifies that you should have robust breach detection, investigation, and internal reporting procedures in place. The idea behind this is that it will facilitate decision-making around an incident, enabling you to quickly gather all available information for when you notify the relevant supervisory authority and the individuals affected by the data breach. GDPR also demands that you keep a record of any personal data breaches, regardless of whether you are required to notify a supervisory authority or not.

If you need help or further guidance around the subject of GDPR, some excellent resources to take a look at are the EU's official GDPR website at https://eugdpr.org and the UK Information Commissioner's Office website, ico.org.uk, which maintains an easy to understand and well-written guide to the General Data Protection Act.

Rule Number Three:
Promptly Notify Those Who Have Been Affected

Nobody likes being the bearer of bad news, but this is your time to reassure the individuals affected by your data breach that you have a best practice plan, that you are working hard to limit the damage, and that law enforcement authorities have been notified of the data breach promptly. Despite the crisis, it is vital that your business is seen as calm-headed, professional, and forthright.

Many experts recommend businesses be transparent in letting the right people know when things go wrong. Here are some ideas for you to think about:

Draw Up a Plain-English FAQ - Lots of security teams like to add a simply written notification FAQ to any breach notification they announce publicly, and it's typically seen as helpful. A plain-English FAQ is helpful because your customers may not be lawyers or technically minded, and they likely will appreciate being able to quickly read clear answers to their most basic questions about the incident and how it directly affects them.

Let Them Know You Have Brought in the Cavalry - Many security teams like to communicate that they have engaged the services of a third-party forensic investigation team to help bolster their immediate response to a cyberattack and the subsequent data breach. Some like to mention the name of the security team or their parent organization, and others prefer to simply say 'a leading cybersecurity organization;' either approach can be helpful, as long as it's true.

Let Them Know You Are Working with Law Enforcement - It is typically helpful to mention that you are working with law enforcement. However, you need to be careful not to detail the status of the investigation or divulge any meaningful information around the law enforcement response to your data breach. Typically, law enforcement officials will provide guidance on how transparent you can be about your case and how and when to provide updates to your employees, customers, and those affected by the breach.

The Devil Is in the Detail - Some teams like to be very specific when they talk about how they were attacked and how their organization was breached, but others are deliberately vague with their language, and that can become frustrating to customers. Sometimes you may not be able to talk about the details, especially if you are working with law enforcement, lawyers, and private cybercrime investigators—the kind of folks who usually have good reasons to ask you not to divulge details. In general, it is important to be as specific as you can with your customers, without compromising trust or pointing fingers at anyone in the process.

Take Ownership - Finding out that you have become the victim of a cyberattack can make your stomach drop, and the notification process may sting more than you thought it would. Even if you've done everything in your power to prevent a data breach, it can still happen. History has shown that, typically, customers and the general public appreciate it when businesses accept responsibility. One way to begin rebuilding trust with your customers is to let those affected see you take ownership of the crisis and act responsibly in the aftermath.

Do You Have Customers in other U.S. States? - All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (businesses, data/information brokers, government entities, etc.); definitions of "personal information" (name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (unauthorized acquisition of data); requirements for notice (timing or method of notice, who must be notified); and exemptions (for encrypted information).

If in doubt, consult the National Conference of State Legislatures' website at ncsl.org for the specific wording of each state's security breach notification laws and obligations.

Typically, most state breach notification laws stipulate more or less the same provisions: you must notify those affected, as well as law enforcement and supervisory bodies, in a timely manner.

Preparing for the Crisis Before It Happens

When cybersecurity breaches happen, being prepared with a well-thought-out Crisis Management Plan is half the battle. You've already taken steps to help maintain business operations and recover lost data from a cyberattack, thanks to your Business Continuity and Data Recovery Plan. Now, you should plan your internal and external communications to minimize reputation damage, and that's where the Crisis Management Plan comes in.

The goal of a Crisis Management Plan is to help prevent a cybersecurity incident from developing into a full-blown crisis. Without preparation and planning, a cybersecurity incident can escalate into a full-blown legal and financial crisis. In crisis management planning, the goal is to establish strategies and procedures that your people can implement before, during, and after a cybersecurity crisis to help mitigate the crisis.

To be ready for a cyberattack when it happens, you should be constantly monitoring the potential threats to your business; you should start building an internal crisis management team so that you are ready as a unit, and finally, you should make sure that the necessary resources are ready when disaster strikes and a real crisis occurs.

Assemble a Crisis Management Team - Taking a broader view of crisis management can help you to properly manage a cyber incident before, during, and after the event unfolds. Many executives see cyber incidents as an IT issue with the IT department being the only group involved, and it is for this reason that the IT department becomes the go-to department in the event of a cybersecurity crisis.

But more effective crisis plans typically involve a coordinated response from multiple departments (operations, compliance, regulatory/legal, public relations, marketing, HR and finance) and draws upon skill sets from across your business when a cybersecurity incident occurs, especially when a cybersecurity incident threatens to escalate to full-blown crisis level.

Because a crisis can impact the business as a whole—its operations, employees, partners, customers, and reputation—your crisis management team should include people from across these areas. It should include senior management to direct the overall crisis operations as well as representatives from operations, customer services, and media relations. Don't forget about including the sales and marketing teams; they should be kept in the loop so they can communicate appropriately with clients.

Develop A Crisis Management Plan - Your crisis management team should have its own cyber crisis playbook, basically a guide to the actions that should be taken in the event of a cybersecurity incident. Your response team's cyber crisis playbook should include specific cybersecurity attack scenarios including web page defacement, theft of company hardware, and a DDoS attack, as well as the obvious data breach and leakage. Determine who will be responsible for what, such as notifying law enforcement and customers. Who will speak for the company, and what will the messaging be? It's best to have a template in place prior to actual crisis time.

This cyber planning is important because it can help prepare your organization to respond to specific threats, and it also informs your people about potential ways to handle cyber incidents to hopefully limit the financial impact and reputational damage to your business. The crisis management team should go beyond a technical response and communicate with the entire organization, from the top down, so everyone is aware of what they should be doing.

It is also to rehearse these training steps and other associated activities on a regular basis, using live drills to make sure that your crisis management team is practiced in delivering a smooth and effective response when crisis calls.

Some Advantages & Limitations of Cyber Insurance

Cyber insurance may sound wonderful, but it can also provide a false sense of security. Do not make the mistake of thinking that cyber insurance is the way to mitigate the risk of a compromise rather than the outcome. Businesses with a low-risk profile often say that they think they can save money by neglecting a real defense in favor of the monetary safety net that is cyber insurance, but this is not a recommended strategy.

While cyber insurance does have benefits and can help you mitigate the costs of a breach, it can have limitations, such as it is often restricted in scope and scale, it can cost increasing amounts of money as breaches increase in frequency, and it probably will never be a comprehensive solution to cybersecurity problems.

The language used to describe cyber risk in underwriting documents and policies can be vague. It's important to completely understand your coverage so that you are fully aware of what incidents are and are not covered.

Continues on page 44

Hack Brief:

Uber Paid Off Hackers to Hide a **57-Million User Breach**

ORIGINALLY PUBLISHED 11.21.17

WIRED

By now, the name Uber has become practically synonymous with scandal. But this time the company has outdone itself, building a Jenga-style tower of scandals on top of scandals that has only now come crashing down. Not only did the ridesharing service lose control of 57 million people's private information, it also hid that massive breach for more than a year, a cover-up that potentially defied data breach disclosure laws. Uber may have even actively deceived Federal Trade Commission investigators who were already looking into the company for distinct, earlier data breach.

On [November 21, 2017,] Uber revealed in a statement from newly installed CEO Dara Khosrowshahi that hackers stole a trover of personal data from the company's network in October 2016, including the names and driver's license information of 600,000 drivers, and worse, the names, email addresses, and phone numbers of 57 million Uber users.

UBER PAID A $100,000 RANSOM

As bad as that data debacle sounds, Uber's response may end up doing the most damage to the company's relationship with users, and perhaps even expose it to criminal charges against executives, according to those who have followed the company's ongoing FTC woes. According to Bloomberg, which originally broke the news of the breach, Uber paid a $100,000 ransom to its hackers to keep the breach quiet and delete the data they'd stolen. It then failed to disclose the attack to the public—potentially violating breach disclosure laws in many of the states where its users reside—and also kept the data theft secret from the FTC.

"If Uber knew and covered it up and didn't tell the FTC, that leads to all kinds of problems, including even potentially criminal liability," says William McGeveran, a data-privacy focused law professor at the University of Minnesota Law School. "If that's all true, and that's a bunch of ifs, that could mean false statements to investigators. You cannot lie to investigators in the process of reaching a settlement with them."

The Hack

According to Bloomberg, Uber's 2016 breach occurred when hackers discovered that the company's developers had published code that included their usernames and passwords on a private account of the software repository Github. Those credentials gave the hackers immediate access to the developers' privileged accounts on Uber's network, and with it, access to sensitive Uber servers hosted on Amazon's servers, including the rider and driver data they stole.

While it's not clear how the hackers accessed the private Github account, the initial mistake of sharing credentials in Github code is hardly unique, says Jeremiah Grossman, a web security researcher and chief security strategist at security firm SentinelOne. Programmers frequently add credentials to code to allow it automated access to privileged data or services, and then fail to restrict how and where they share that credential-laden software.

"This is all too common on Github. It's not a forgiving environment," says Grossman. He's far more shocked by the reports of Uber's subsequent coverup. "Everyone makes mistakes. It's how you respond to those mistakes that gets you in trouble."

THE NAMES, EMAILS, AND PHONE NUMBERS OF **57 MILLION UBER USERS WERE STOLEN**

Who's Affected

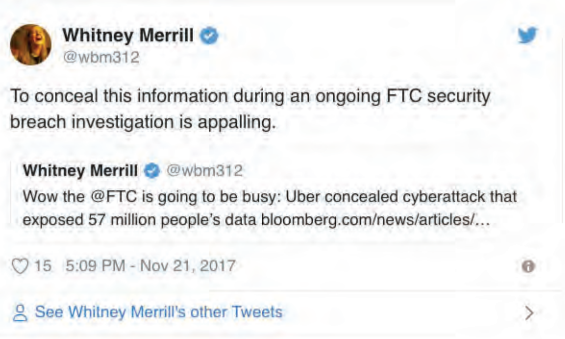
Uber's count of 57 million users covers a significant swath of its total user base, which reached 40 million monthly users last year. The company hasn't notified affected users, writing in its statement that it's, "seen no evidence of fraud or misuse tied to the incident," and that it's flagged the affected accounts for additional protection. As for the 600,000 drivers whose information was included in the breach, Uber says it's contacting them now, and offering free credit monitoring and identity theft protection.

How Serious Is This?

Mass spills of names, phone numbers, and email addresses represent valuable data for scammers and spammers, who can combine those data points with other data leaks for identity theft, or use them immediately for phishing. The more sensitive driver data that leaked may offer even more useful private information for fraudsters to exploit. All of it contributes to the dreary, steady erosion of the average person's control of their personal information.

But it's Uber, not the average user whose data it spilled, that may face the most severe and immediate consequences. The company has already fired its chief security officer, Joe Sullivan, who previously led security at Facebook, and before that worked as a federal prosecutor. By failing to publicly disclose the breach for over a year, the company has likely violated breach disclosure laws, and should be bracing for hefty fines in many states where its users live, as well as its home state of California, says the University of Minnesota Law School's McGeveran. (In statements on Twitter embedded above, former FTC attorney Whitney Merrill echoed that interpretation of those breach disclosure laws.) "I would not be surprised to see states pursuing Uber on that basis," McGeveran says.

Former FTC attorney Whitney Merrill echoed that interpretation Tuesday on Twitter:



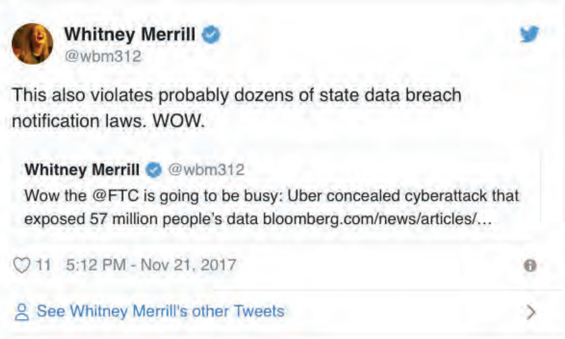
Whitney Merrill @wbm312

To conceal this information during an ongoing FTC security breach investigation is appalling.

Whitney Merrill @wbm312
Wow the @FTC is going to be busy: Uber concealed cyberattack that exposed 57 million people's data bloomberg.com/news/articles/…

15 5:09 PM - Nov 21, 2017

See Whitney Merrill's other Tweets



Whitney Merrill @wbm312

This also violates probably dozens of state data breach notification laws. WOW.

Whitney Merrill @wbm312
Wow the @FTC is going to be busy: Uber concealed cyberattack that exposed 57 million people's data bloomberg.com/news/articles/…

11 5:12 PM - Nov 21, 2017

See Whitney Merrill's other Tweets

If the cover-up included making false statements to the FTC during its investigation of the 2014 breach—even though it was a separate incident—that could have even more dire consequences. Making false statements to the commission's investigators, McGeveran points out, is a federal criminal offense. "This is not just a casual chat over a cup of tea. It's a formalized investigative procedure," McGeveran says. "They're already being asked investigative questions by a government official. They not only know about the breach, but they're allegedly paying hackers to cover it up. They presumably omit this 57 million person breach from their disclosure to the FTC."

"If all of that is true," McGeveran reiterates, "that's huge."

Continued from page 40

Because payouts are often capped, premiums are typically expensive, especially for vulnerable industries, and cyber insurance is not generally a comprehensive solution, it may not be cost-effective enough for your small businesses to consider. But, if you employ lots of people, you should consider investing in some cyber insurance coverage. Just don't make the mistake of thinking that it replaces employee cybersecurity training and good cybersecurity planning.

When to Consider Cyber Insurance?

If your business handles any kind of personally identifiable information like health insurance records, medical information, financial information on customers or online account information, such as security answers and questions, passwords, email addresses, it is strongly recommended that you consider it. If your business collects any kind of data or even if you are heavily reliant on email communications with your customers, then you should also consider cyber insurance.

As with any other kind of insurance policy, the idea with cyber insurance is to mitigate cyber-related risk and potential financial loss. Generally speaking, if you have cyber insurance in place, then you will benefit from several offerings.

You Get A Crisis Management Partner - If your business does experience a data breach, then your cyber insurance company will begin to behave like a crisis management partner. They will start to help you minimize the financial impact on your business and those individuals and organizations most affected by the breach. It minimizes their own exposure in the process.

The Application Process Is Important - The application process to secure cyber insurance is more intensive than most liability insurance in that it can be quite detailed. Your insurer will request enough information from you to comfortably evaluate the potential risks associated with your operation and establish a level of risk that will dictate your insurance premiums. The process itself brings light to potential cyber risks. Proactively remediating any concerns raised by your insurer during the application process can help lead to lower premiums and help fortify your overall cybersecurity posture.

Business Impersonation

Even though almost everyone has heard of identity theft before, it can still be a shock when you discover that your business is being impersonated by others for criminal purposes. Remember those phishing emails from the first section? They typically impersonate a legitimate business to gain credibility with the potential victim. What if that legitimate business is yours?

You may have noticed recently that many large corporations have stopped sending account links through emails; this is a preemptive strike against email scams. They inform their customers that they will never send emails containing links—rather they will request customers log in to their accounts separately to take action—and therefore, customers should be wary of any email that appears to be from them that contains links. If your business can set up a system like this, you'll be in a better position to protect yourself from impersonation.

If you become aware that someone is impersonating your business, here are a few steps to take to help protect your reputation and reclaim your business's identity:

- Notify your customers as soon as possible. Announce the scam on your business's social media accounts, and warn customers to be wary of emails or texts that claim to be from your company. You should also send out emails and possibly letters warning your customers of the scam.
- Contact law enforcement. Report the scam to the FBI's Internet Crime Complaint Center at ic3.gov and suggest to your customers that they forward any phishing emails to the Anti-Phishing Working Group (antiphishing.org), a public-private partnership against cybercrime. Finally, consumers also can file a complaint with the Federal Trade Commission through ftccomplaintassistant.gov.

Quick Wins for website security.

CREATE A SAFE ONLINE SHOPPING EXPERIENCE FOR YOUR CUSTOMERS.

- Keep software up-to-date
- Require users to create unique, strong passphrases to access
- Prevent direct access to upload files to your site
- Use scan tools to test your site's security – many are available free of charge
- Register sites with similar spelling to yours
- Learn More: ***https://bit.ly/2OJZVOe***

CYBER DEFENSE FOR SMBs

HOW ARE YOU GOING TO KEEP YOUR BUSINESS **#CyberSafe** in 2019?

Congratulations, you should now have a better understanding of the cybersecurity fundamentals for your business! You have a better idea of what data you are collecting, where you store it, and how it is protected. You have a plan in place to help maintain business operations should a cyberattack take your computer network offline. You have a plan to help your business respond to and recover from a cyberattack or data breach. And you know some steps to take to improve your cybersecurity further over time.

Now comes the truly important part: implementing these changes, enforcing the new guidelines, and making cybersecurity a regular part of your business planning moving forward. One thing that will help tremendously with these next steps, and in improving your overall cybersecurity posture, is employee training.

As stated earlier, most cybersecurity experts agree that employee awareness training is the single best investment in cybersecurity you can make for your business. Employees are your first line of defense, and creating a culture in which cybersecurity is taken seriously and implemented throughout the workplace will go a long way to helping your business avoid becoming a victim. To learn more about free employee training resources for your business, visit **cyberflorida.org/SMB**.

We hope you have found this guide informative and useful and feel more empowered to take control of your business's cybersecurity. Connect with us through cyberflorida.org, and follow us on social media for news on events, new threats, and new solutions.

Remember, when in doubt, DON'T CLICK!

Sincerely,
The Cyber Florida Team
info@cyberflorida.org
cyberflorida.org/SMB

@cybersecurityfl

floridacyber

@cybersecurityfl

cyberflorida

Data Protection Best Practices

The tips outlined here represent a basic level of "good" cybersecurity. Use these protocols to help determine your baseline security posture and where you can improve.

Note: *Cyber Florida cannot recommend specific products or services. To help determine if a product or service is right for your business, please seek assistance from an unbiased third-party service that provides testing and reviews of products or services or seek the assistance of a qualified professional.*

End-User Computer Security

Protect against viruses, spyware, and malware.

Make sure all of your business's computers are equipped with antivirus and antispy software and updated regularly. Configure all software to install updates automatically. If you are using a Windows operating system, enable the Windows firewall to the highest setting and turn on Windows Defender.

Update the BIOS.

BIOS stands for basic input/output system. Embedded on the computer's motherboard from the factory, the BIOS provides instructions for the computer's basic functions, such as starting up (booting) and keyboard control. The BIOS need to be kept up-to-date as well (even on a new computer). Visit the computer manufacturer's website support page for instructions on updating the BIOS.

Control physical access to computers and network components.

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee, and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel. Keep servers and backup data under lock and key.

Establish security practices and policies to protect sensitive information.

Establish policies on how employees should handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating your business's cybersecurity policies.

Require employees to use strong unique passphrases.

The latest password wisdom is that a *passphrase* of at least 16 characters is considerably more secure than a password. Length is key. Incorporating numbers and symbols adds to the security. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. See Password/Passphrase Tips to learn more.

Restrict access.

Keep your customers' sensitive data safer by restricting access to only those necessary. Set up user accounts for your employees, and only grant permission to access sensitive data to those who absolutely need it. Check the software manufacturer's website for instructions on restricting access and setting up user accounts.

Create a mobile device policy.

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Employ (and enforce) a Mobile Device Policy that outlines the security measures required of all devices you allow on the network. Visit cyberflorida.org/SMB for some sample Mobile Device Policies. Consider employing a third-party Mobile Device Management (MDM) solution, which can ensure that networked devices conform to your Mobile Device Policy standards and warn of any risky devices.

Don't connect unknown USB drives.

If you must connect an unfamiliar device, right-click and scan it before opening any files.

Wi-Fi and Network Security

Secure your networks.

Visit your router manufacturer's website for instructions on enabling the firewall (if equipped), updating the password, and other router security protocols. If your router does not come with a firewall, consider upgrading to one that does. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

Make backup copies of important business data and information.

Regularly backup the data on all computers. Critical data includes customer databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly, and store the copies either offsite or in the cloud. For added protection, encrypt your backups (most backup media and cloud storage solutions offer encryption).

Use separate Wi-Fi for guests and customers than you do for business.

Don't Forget the Printers.

Digital copiers, printers, and fax machines are computers, too, and represent a point of entry into your network. Ensure that these devices employ encryption and overwriting.

Point-of-Sale Security

Employ best practices on payment cards.

Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor. Create separate administrator and user accounts and isolate payment systems from other, less secure programs. Do not browse the web on POS terminals.

Website Security

Protect all pages on your public-facing websites, not just the checkout and sign-up pages.

Speak with your website hosting company to ensure basic security precautions are in place. Your site URL should start with HTTPS—Hyper Text Transfer Protocol Secure—which means that all communications between the browser and the website are encrypted. Additional layers of security, such as SSL/TSL (Secure Socket Layer/Transport Layer Security) should be employed as well on sites where people make purchases.

Password/Passphrase Tips

Select a passphrase that is easy for you to remember but difficult for others to guess.

- The phrase should be at least 16 characters, but the longer, the better.
- Numbers, symbols, and uppercase and lowercase letters may be incorporated, but the length is key.
- Do not use birthdays, children's names, pets' names, or any other information that is easily discoverable or well known about you.
- Do not use common, bad passwords such as 'password,' '123456,' 'qwerty,' etc.
- Select four or five seemingly random words that have personal meaning or a statement such as, **'pepperonipizzais100%lit.'**

Sources: U.S. Small Business Administration, National Cyber Security Alliance, the U.S. Federal Trade Commission, NIST

This guide is made available by the Florida Center for Cybersecurity for general educational purposes only and should not be used in lieu of obtaining competent legal advice from a licensed attorney and/or cybersecurity professional with the sufficient expertise necessary to address your organization's specific needs. Use of this guide does not create any special or fiduciary relationship between you and the Florida Center for Cybersecurity or the University of South Florida.

CYBER
FLORIDA
at the **UNIVERSITY OF SOUTH FLORIDA**

CYBERFLORIDA.ORG | 813-974-2604 | 4202 E. FOWLER AVE., TAMPA, FL 33620

CYBER
DEFENSE
FOR SMBs