an overview of cybersecurity fundamentals by **CYBER FLORIDA**

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

CYBERSECURITY

FOR LOCAL GOVERNMENT

Dear Reader,

It is not hyperbole to say that cyberattacks have become pervasive in our society. Practically every week, we hear about another business, organization, or government suffering a cyberattack. Cybercriminals are prolific and continuously developing more sophisticated tactics.

Recent news of cyberattacks against small municipalities, school districts, and other local government entities have highlighted the vulnerability of these organizations. Government entities maintain a host of valuable data, but smaller jurisdictions do not necessarily have the resources to combat ever-evolving cyber threats and the tenacious, well-organized criminals behind those threats.

This reality prompted Cyber Florida to partner with the University of South Florida School of Public Affairs, the Florida League of Cities, the Florida City and County Management Association, and the Florida Local Government Information Systems Association to examine the challenges facing local government organizations and learn how we can work together to mitigate those challenges.

First, we surveyed a sample of Florida's city and county governments. Titled, "Cybersecurity: Are Florida's Local Governments Prepared?" the survey report shares input from 101 jurisdictions across Florida—mostly small municipalities. The responses indicate, as we suspected, that many small local governments are indeed aware of the need for robust cybersecurity, but lack the resources needed to implement stronger cybersecurity practices.

Next, we used the responses to help determine the content of this guide and have shared some of the survey data where relevant. This guide is an effort to help educate local government leaders on some of the foundational best practices of cybersecurity. We hope that it will help you build familiarity with the concepts and practices at the core of cybersecurity and empower you to better plan and prioritize resources to help reduce their risk of your organization becoming a victim of cybercrime.

Sincerely,

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

Table of Contents

Part One: Threats

Part Two: Best Practices

Part Three: Crisis Management

This guide was produced in partnership with the University of South Florida School of Public Affairs, the Florida League of Cities, the Florida City and County Management Association, the Florida Local Government Information Systems Association.

Part One: Threats

WHO PERPETRATES CYBERCRIME?

Cyberattacks against government entities are becoming more frequent and sophisticated. Compared to just a decade ago, cyberattacks have become pervasive, and cybercriminals do not confine themselves to attacking only large organizations. Increasingly, cybercriminals are targeting local government entities because they know that these types of organizations are less likely to have the resources and security infrastructure in place to prevent or mitigate an attack as successfully as their larger counterparts. In other words, you may think your jurisdiction is too small for a cybercriminal to bother with but, to cybercriminals, a small town may be an easy and valuable target.

Who is behind these cyberattacks, and what is their motivation? The most prolific type of cybercriminal is the malicious outsider, a criminally minded individual or group whose primary goal is financial gain or intellectual property theft. However, these malicious outsiders often employ tactics that involve manipulating authorized users to install malware or relinquish login credentials inadvertently, a process called 'social engineering.' These unwitting accomplices can play a critical role in the success of the malicious outsider's attack, making them a significant threat on their own, known as an insider threat. The combination of malicious outsiders and unwitting insiders is responsible for many successful cyberattacks.

The malicious insider can also pose a threat. Disgruntled current and former employees might seek revenge through a cyberattack. Some may abuse their access for financial gain, stealing data and selling information "on the side."

Other types of attackers that frequently target government entities include hacktivists, that is, people who target organizations involved in controversial affairs, and state-sponsored operators (i.e., foreign spies) who attack organizations to conduct espionage and/or sabotage or simply to disrupt a foreign adversary.

Let's take a closer look at the most common types of cybercriminals targeting government organizations.

COMMON CYBER THREAT ACTORS

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

Hacktivists: A 'hacktivist' is a hacker with a cause. They will try to infiltrate your organization because it engages with an industry or in a practice that they disagree with, so much so that they are willing to commit a crime to disrupt or damage an organization. Hacktivists often deface websites with political messaging and contact customers or constituents to tell them of an organization's supposed wrongdoing. They may also steal and release data, but it's less likely that they will do so for financial gain and more likely to affect organizational reputation. Government entities, in particular, can fall victim to hacktivism due to the often-political nature of the work they perform.

Phishers: Phishers also fall into the malicious outsider category and employ social engineering tactics to gain entry. They send 'phishing' emails, so named because they are designed to *fish* for login credentials and other information. Typically, they pose as a legitimate service, vendor, or business partner that you may use and email you with an account maintenance alert message, urgent password reset notice, or overdue invoice. Unfortunately, even with constant training, phishing emails can sometimes fool the best of us.

Phishers are probably the most common threat and the most common kind of cyberattack that your organization is likely to encounter. They are also among the most difficult to stop because phishers use sophisticated tactics, typically

pretending to be somebody the user knows and even emailing from an address that the user recognizes through a process called spoofing. The email typically directs the user to a website that is probably doing a great job of posing as a legitimate online service but is really a false front designed to capture the user's login credentials.

Government organizations may find themselves the victim of phishing for all the reasons other types of business verticals do with the added caveat that the trust associated with a government email addresses makes them valuable to use for phishing others. For example, every tax season sees an influx of phishing emails and texts that appear to come from the U.S. Internal Revenue Service targeting taxpayers, accountants, payroll specialists, and human resources representatives to steal login credentials and personally identifiable information (PII).

Malicious Insiders: Malicious insiders are usually disgruntled employees intent on causing damage to your IT infrastructure. Public safety agencies, however, that have access to criminal justice or health information may fall victim to unscrupulous insiders motivated by financial gain or personal reasons. 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.

WHAT ARE THE MAIN TYPES OF CYBERATTACKS?

There are four main types of cyberattacks, known as the **Four Ds: Data loss, Disruptive, Destructive, and Disinformation.**

Data Loss or Exposure: Data loss or exposure, also known as data breach, is quite possibly the most damaging cyberattack, depending on the importance of your data. Due to Florida's more transparent public records laws, data breach is not as much of a concern for Florida public entities. A business, however, has much to lose if its customers' personal, financial, or other data becomes exposed due to a cyberattack.

Disruptive: This type of attack is designed to disrupt or impair your organization'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 the organization's data and demand a (usually small) ransom to decrypt it, severely restricting the organization's ability to operate until they pay the ransom. This type of attack can last days or weeks, and an unprepared organization may find themselves with no choice but 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 the organization's website, causing the site to crash and disrupting business operations.

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

Another form of destructive attack that has been used to target public officials and government employees is known as 'doxxing.' The term stems from the word 'documents' and refers to the practice of collecting private documents and personal information on someone, sometimes through illegal means and sometimes through diligent research, then sharing that information online in an effort to discredit or embarrass a person or organization.

Disinformation: Disinformation attacks spread false information about a person or organization's activities and employees to inflict reputational, financial, and even legal damage. Malicious disinformation about an organization can spread quickly through many different social and digital channels, much faster than one can counter or have it removed. A sustained campaign can inflict serious damage on an organization, even if none of it is true, and in many cases, you have no real idea of who is behind it—malicious insiders, hacktivists, or state-sponsored actors.

HOW ARE ATTACKS CARRIED OUT?

Before we examine how cyberattacks are carried out, we need to understand the "attack surface," which is a professional term used to describe the collection of devices, hardware, and software that compose an organization's IT infrastructure. The

FROM THE SURVEY

48% of respondents have suffered a malware attack in the past three years.

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 applications that connect to your organization's network can serve as the point of entry for an attacker and is a part of the attack surface.

Government organizations often possess wildly complex network and data structures, creating a diverse and disparate attack surface. Boundaries between organizations that are relatively obvious in a practical sense may not be so in a technical sense. Any government organization's systems are almost certainly part of a larger government ecosystem. This complexity poses challenges and opportunities both for attackers and targets.

There can be numerous avenues for a hacker to find a way into your IT infrastructure. While some 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 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 organization.

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. This kind of attack is difficult to defend against because it focuses on the individuals in your organization 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.

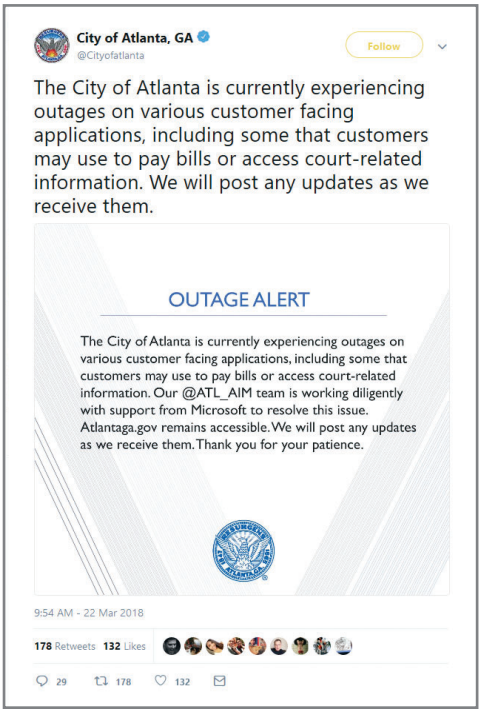
A major concern with social engineering is that you could have all the latest cybersecurity tools in place to protect your organization and still fall prey to these techniques because the weakest link in any organization's attack surface is people. Social engineers can be incredibly effective at getting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

Government organizations have the additional challenge of defending against social engineering attacks while navigating various government record laws. Government employees must protect sensitive information about their networks and systems while also adhering to public record law. Generally speaking, government documents are public records, and members of the public may request them with no verification requirement. These requirements vary by state, and in Florida, certain information that may expose a security vulnerability could be exempt from public disclosure in certain cases. It is important to understand the legal exemptions as they pertain to your jurisdiction to allow your employees to resist social engineering attempts and follow public record laws. Many organizations address this issue by appointing a public records officer who has the responsibility of reviewing requests and working with legal counsel to redact any exempted information in a timely and reasonable fashion.

Phishing Attacks: Phishing, a type of social engineering attack, is probably the most common type of cyberattack against government entities and involves the extraction of personal information and login credentials from users by means of deception. Phishing emails are designed to look like they come from a reputable service provider and often include a reasonable yet urgent request to attend to an account issue such as an overdue invoice. Clicking on the link in a phishing email takes the victim to a website that looks almost identical to the service provider's actual site, hoping to trick them into

Case Study: Atlanta Ransomware Attack

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. The ransomware, which likely entered the system by means of a brute-force attack (i.e., correctly guessing a weak or default password), disrupted court scheduling, shut down online utility payments, caused the public WiFi at the nation's busiest airport to go offline for two weeks, and destroyed decades of municipal correspondence as well as footage from police dashboard-mounted cameras. The cybercriminals demanded the city pay a ransom of $50,000 in Bitcoin. 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 $2.6 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. Cybercriminals typical set the ransom at an amount they think their victim can afford to make it the more cost-effective option. For many organizations, a sustained outage of their IT services can have serious consequences and, as was the case for Atlanta, emergency spending on cybersecurity cleanup efforts can far outweigh the cost of ransom.

The City of Atlanta, however, will undoubtedly benefit over the long term by choosing not to pay the ransom and instead investing in professional remediation–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.

entering login details or other 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 run-up to the 2016 presidential election. More commonly, though, these attacks are used to prey upon organizations and individuals for financial gain.

Phishing emails may also contain file attachments intended to infect your device with malware. Sometimes they will try to gain the user's trust by including some personal information that makes them more inclined to believe the email is legitimate, a tactic known as 'pretexting.' This scenario is often the method used to begin a ransomware attack.

Malware Attacks: Malware is an umbrella term for all types of malicious software, from worms and viruses to spyware and ransomware. Two common sources of malware infection for an organization are employees visiting websites and clicking on malicious links and employees engaging with phishing emails, clicking links or opening attachments. Once malware gets a foothold, it can be difficult and expensive to remove.

Examples of malware include the following:

Remote Access Trojans: Allows the attacker backdoor entry into systems.

FROM THE SURVEY

Less than 30% of respondents provide their external vendors and contractors with cybersecurity standards.

Ransomware: Encrypts data until a ransom is paid.

Spyware: Logs keystrokes to gather data such as passwords.

Adware: Exposes the victim to potentially malicious ads.

Worms: Self-replicates, spreading without user interaction.

Viruses: Infects other files, making cleanup difficult.

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

Point-of-sale (POS) Intrusions: If your jurisdiction uses a POS system to process citizen transactions, it may be vulnerable to POS-specific cyberattacks. Commonly, hackers breach POS systems via the remote access points that POS 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 citizens' transactional and credit card data for months, years, or as long it takes for you to detect them.

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 design flaws in the hardware or software, manufacturing defects, 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. A talented (or lucky) hacker may find that you have operating systems that are not up to date, have not updated a software application, or have an unsecured remote access point intended for support technicians.

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

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. Hackers typically reserve zero-day attacks 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. Government information security professionals may find themselves facing zero-day attacks due to the value of the information they protect.

THIRD-PARTY & SUPPLY CHAIN RISKS

It's not just your organization's security that you have to worry about; you must also consider threats stemming from third-party vendors and your supply chain. A supply-chain cyberattack occurs when criminals infiltrate an organization's IT systems through a partner or provider that already has access to the systems and data. As governments often rely on third-party vendors to collect payments, fees, and taxes, it is essential that these vendors maintain adequate security protocols.

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 added to the supply chain, the greater the chance that your organization will become the victim of a cyberattack via that channel.

According to the National Institute of Standards and Technology (NIST), 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.

Learn more about the NIST Cybersecurity Framework and supply chain management best practices here: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management. Additional resources for local governments are available from the Cybersecurity and Infrastructure Security Agency (CISA) here: https://www.us-cert.gov/resources/sltt. You can also access these resources at cyberflorida.org/gov.

While it is not always possible to enforce security standards on third parties, being aware of potential risks and being judicious when choosing partners can go a long way toward maintaining a secure supply chain. Consider documenting your jurisdiction's cybersecurity protocols and require that they maintain, at a minimum, the same protocols.

Case Study: Click2Gov

In September 2018, the networks of at least 46 U.S. municipal governments were compromised after personal data from Click2Gov, a third-party vendor, was breached. Click2Gov is an online billing portal developed by Superion, which citizens can use to pay for government services such as utilities, parking tickets, and civil citations.

Reports of Click2Gov vulnerabilities first surfaced in 2017, and over a year later it was confirmed that malicious software had infected the server and breached the credit card information of approximately 294,929 people throughout the U.S. and Canada. Despite the third-party software's security precautions, cyber attackers utilized an undetected (zero-day) vulnerability to hack into the server and extract the personal data of customers who had used the online system to make payments between August 11 and September 25, 2018.

The data breach compromised several Florida cities, including St. Petersburg, where approximately 28,000 customers' credit card information were exposed. City officials immediately responded to the breach by shutting down the online payment system and offering advice to citizens who felt they were at risk of identity theft, and a new system was built and fully operational the next day.

Third-party software vendors are prime targets for cyber attackers. It is recommended that companies and governments that use third-party vendors actively update the software and frequently monitor their networks to reduce any system vulnerabilities that may be targeted by cybercriminals.

Part Two: Best Practices

A good first step toward improving cybersecurity for your jurisdiction is to examine what is known as your cybersecurity 'posture,' meaning the current state of your organization's cybersecurity, also known as conducting a risk assessment. The following pages review some of the basics of conducting a cybersecurity risk assessment. Additional resources and more in-depth procedures can be found within the NIST Cybersecurity Framework, under the "Identify" category, here: https://www.nist.gov/cyberframework/identify.

Step One: Audit Your Data

One way to begin a cybersecurity risk assessment is to conduct a thorough data audit. As a public servant, you are responsible for the security of the data you gather and maintain, and you can't secure what you don't know you have.

Begin by asking yourself and your staff some difficult questions. What data are you collecting by design or by accident? Where do you store that collected data? For how long do you store it? How do you protect it? Write all the answers down, then go back and reconsider the 'by accident' part and try to think of anything you may have missed. Ask yourself, "If this were my personally identifiable data, would I be comfortable with the level of protection in place?" If you've never done this before, it is highly likely you will discover some unprotected data, and that's okay. For many organizations, technology and digitization of data simply have outpaced their ability to secure that data. What matters is that you are taking some steps toward improvement.

WHAT IS YOUR DATA?

Download the Data Audit worksheet at cyberflorida.org/gov to make a list of the data that you know your jurisdiction collects. Include the data you hold in your citizen database system and accounts payable and receivable. Do you use point-of-sale (POS) machines to process credit cards? Also look for website visitor tracking information, social media analytics, and email marketing data and add those to the list.

Do you have any old Excel spreadsheets hidden away in a hard drive or filing cabinet? Add that to the list as well. Payroll and HR files? Very sensitive data for the list. Finally, let's not forget about the third parties who may hold your jurisdiction's data on your behalf: suppliers, vendors, and contractors. If they have some of your citizen 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?

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

Talk to the Team

Though you have managerial oversight, you may not be aware of everything your team does with your jurisdiction's data. Be sure to talk to your team and ask them about the data they handle so that you can add it to the list. Talk to key staff members and leave no stone unturned. Employee data handling practices are a blind spot for many organizations. Leaders think they know their organization's data flow, but employees often create alternative work flows and might be handling data in ways you don't realize. Including your employees in this process also lets everyone know that you take cybersecurity 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 that which may be an attractive target for cybercriminals, such as credit card information, as well as that which is critical to organizational operations.

Government entities, for example, might consider information that is exempt from Title X, Chapter 119, of the Florida Statutes, such as sealed bids and active criminal investigative information, as high-value data as well as any assets that are necessary to ensure ongoing operations.

Rank all your data in terms of value to your jurisdiction. Once you know exactly what your high-value data is and where it lives, your data audit is nearly complete—a huge first step on the road to better 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.

It is also a good time to think about passwords. How strong are the passwords used to secure your data? How often are passwords reused across the organization, and how frequently are passwords changed?

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 organization. The next step is to consider the threats unique to your jurisdiction.

Step Two: 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 we 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 definitely will try to rob you because you store boxes of expensive electronics in your warehouse. You need to put bars over the windows and locks on the doors. You should also install an alarm system and maybe get a guard dog." That, in a nutshell, is threat modeling.

Create a threat model for your jurisdiction. The goal is to reduce your attack surface, meaning the number of potential entry points that an attacker can use to enter your organization. An entry point could be a shared password, citizen 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.

To craft a threat model for your jurisdiction, begin by answering these questions:

What Is It That We Do?

Through the eyes of an attacker, meaning if a criminal looked at your organization, what is it that you do that s/he would find of interest? Government entities may possess citizen information, health records, criminal justice records, and intellectual property, all items on the cybercriminal wish list.

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 to your systems, 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 a 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 system if you were a criminal. Where would you start first? Where do you think that your 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—possible backdoors and weaknesses that a cybercriminal could exploit.

It 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 organization, 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 another employee. We often hear about hackers pretending to be IT support technicians and tricking employees into giving them their passwords. Social engineering is a very real threat and another reason to invest in employee training.

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? It's convenient, but perhaps everyone should have a unique 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 for your organization. Refer to the Data Protection Best Practices section for guidance on some actionable steps that you can choose to implement right now that are likely to improve your cybersecurity posture.

How Did We Do?
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 organization, and you can use that improved understanding to develop and hone your cybersecurity awareness and practices over time.

Step 3: How Much Security Is Enough?

It is a difficult question to answer for any organization. Industry standards will be reviewed in the "Good, Better, Best" section, but ultimately, it comes down to each jurisdiction to determine what an adequate level of security is, given the financial resources available. What is the value of the property or data at risk, and what potential consequences might stem from a successful cyberattack?

For example, due to Florida's open public records laws, much of the data maintained by local governments are considered public information, and therefore a data breach exposing those records is not as serious an issue as it would be for a private business, which is expected to maintain customer privacy. However, a cyberattack that destroys or otherwise renders that data and equipment unusable, such as in a ransomware attack, could wreak havoc with basic jurisdictional operations. In that case, one might prioritize investment in a robust backup system to help ensure an easier and more complete recovery in the wake of a cyberattack.

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

1. To sustain operations, what needs protecting? Consider information, technology (hardware, software, or systems), networked equipment, facilities, and employees.

2. What could happen if it's not protected? Try to envision all the potential impacts of a cyberattack. How are systems connected? What if the phone system stopped working? Traffic signals? 911? How would you communicate with your jurisdiction if your website crashed?

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

FROM THE SURVEY

35% of respondents do NOT require new employees to receive basic cybersecurity training.

Case Study: District 129

After West Aurora Public School District 129 ("District 129"), fell victim to a series of cyberattacks that resulted in a security breach in 2016, district officials determined that a greater emphasis on cybersecurity was necessary to ensure that student and faculty data remain protected. Acknowledging a lack of cyber awareness and proper training as the main causes of the attacks, the Illinois school district created a customized security awareness program with KnowBe4 to improve end-user training and educate employees on properly mitigating cyberattacks, specifically phishing emails. Over the course of five months, District 129 engaged in various simulated tests and training exercises to create a more security-aware culture among staff, eventually reducing the district's monthly "phishing-prone percentage rates" from 27% to .03%.

You can spend a lot of money on firewalls and technology, ***but there's no device that's going to make you safe from phishing.*** *The only way you can be as safe as possible is to make sure employees and end-users know what they are doing."*

Don Ringlestein, Director of Technology, West Aurora School District 129

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 an organization's cybersecurity strategy, primarily because many organizations neglect to invest resources in employee training, even as they spend money on other cybersecurity measures.

Protecting Your Data: Good, Better, Best

The "good, better, and best" approach 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.

Good (Protect/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 action items listed in the Data Protection Best Practices section can help guide you toward good security practices.

Better (Detect/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. Monitoring 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) to 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 citizens.

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 can apply 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. Similarly, Florida Administrative Code 74-2: Information Technology Security (https://www.flrules.org/gateway/ChapterHome.asp?Chapter=74-2) also conforms to 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 in which every organization should engage 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 A SPECIALIST?

If your jurisdiction cannot afford to hire personnel devoted specifically to cybersecurity or to 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 local government's cybersecurity can be a worthwhile 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. They may be able to spot things you may have missed and make technical recommendations.

If you do have some resources to invest in cybersecurity, you may be thinking about hiring an internal security person or bringing in a vendor to help you. But how to choose?

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 costly; however, they typically have a lot of experience and resources and are actively 'plugged in' to the current threat landscape. Additionally, many cybersecurity firms are aware of the budgetary restrictions faced by local governments and will offer competitive pricing.

When you hire an employee, you get a core member of your team managing your security, one who will become intimately familiar with your organization's people, processes, and technology. Such expertise can come at a high cost, but if you would like to move your organization 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

FROM THE SURVEY

51% of respondents outsource some or all of their cybersecurity operations.

leaders, evangelists, and freelancers who sound like they speak a foreign language to the average person. It can be intimidating to speak to an expert about such an esoteric topic, but a quality service provider should be able to discuss cybersecurity in easily understandable terms.

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 or employee. They should be able to explain security risks and processes to you in plain English, and analogies are a good 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.

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 organization 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: Some consultancies will send one of their senior practitioners to come and talk to you and convince you that you are in good hands. But when it comes to performing the work, they may send a junior employee or beginner with minimal 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 if they have good supervision.

Ask them about their mistakes: Good cybersecurity professionals can adequately evaluate your security risks and penetration test your networks without bringing your 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. 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: Consider both their industry certifications and practical experience. Many legendary cybersecurity practitioners 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 valuable, and a good potential candidate will have some real-world experience on their resume.

Ask them if they will train your employees: It is essential that the consultant answer this question correctly with a resounding, "YES!" Some consultants think that employee training is beneath them; those who feel that way are doing your organization 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

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 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 a response and recovery plan in place. Making your organization more cyber resilient means you will be better prepared to weather a cyberattack with minimal disruption and data loss.

Case Study: Cloquet School District

Two years after the Minnesota-based Cloquet School District was hit with a ransomware attack that infected district servers and more than 600 computers, district officials discovered that their servers had once again been targeted by ransomware. Fortunately, the previous attack ensured that district members were more prepared to mitigate a future crisis without being forced to pay a ransom to the attackers. Board members of Cloquet School District decided to recreate the encrypted data and rebuild affected servers rather than paying for their encrypted files, building a stronger cyber defense system and reducing the district's probability of being targeted again in the future.

Imagine the worst-case scenario: say your jurisdiction came under a ransomware attack from a 15-year-old hacker calling himself Pharaoh Snefru. Young Snefru has recently discovered the wonderful world of ransomware-as-a-service (RaaS)—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 public information officer, 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. 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 your 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 organization objectively and roughly determine a ransom appropriate for your resources. He demands $1 million.

Even worse, he is on social media boasting about his 'achievement' while the ransomware not only encrypts data, but also the software running your phone system and your website's content management system.

Snefru has told all his friends about his exploits, and they are egging him on and abusing your jurisdiction 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 citizens have noticed, and they start using all caps, too.

That is just about the worst cyber disaster that one can imagine, and it really happened. While this particular scenario happened to a small business, it could just as easily have been a small municipality. 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 cyber resilience and can help keep your business functioning during a cyber crisis.

Here, the focus is on the 'recover' aspect of the NIST framework ('respond' is the focus of the next section). If your jurisdictional operations are disrupted, it can cost real money. If you lose any revenue and your costs increase, it may have a severe impact on your jurisdiction's budget, and insurance may not fully cover losses. You should have a well-thought-out business continuity and disaster recovery plan in place.

1. Determine which part of your organization's 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 planning are needed now to keep operations running

FROM THE SURVEY

20% of respondents reported that their jurisdiction does not have a cyber incident response plan and of those that do have a plan, only 22% have tested it.

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 staff and conduct mock disaster exercises to make sure that your plan and your people know what to do. Many organizations get as far as Step 3 but stop short of Step 4. Your plan is not complete until you have tested it.

Determine Which Business Operations Are Critical: In the industry, this step is called an 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 Impact Analysis worksheet at cyberflorida.org/gov to help you with this. You should complete one of these for each department you have, which likely will build a better mission-critical picture and properly prioritize the impact risks. Public safety processes and functions with the highest financial and operational impact are likely the ones that you will want to restore first.

Determine How to Support Recovery Activities: Recovering 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 Plan worksheet at cyberflorida.org/gov to help with this. Each of your department managers should fill one of these out so that you have a better view of the resources and time you may need to recover your operations. These resources could be people, technology, important records, utilities (electricity or internet), and 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 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. Detail the aspects of your operations that are vitally important and how much time you have to restore those functions should disaster ever strike.

In short, you should plan your recovery strategies. If your organization is hacked or your data is encrypted by ransomware, you should have a plan that will tell your continuity team exactly what to do. It could be anything from relocating your key staff to a backup facility 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 staff so they know what to do and where to find answers. Many experts advise running these exercises at least once a year, and while you are doing so, validate 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 organization quickly respond to and recover from a cyberattack. Remember the words of Benjamin Franklin, "By failing to prepare, you are preparing to fail."

Part Three: Crisis Management

John Chambers, the 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." Cybersecurity experts often quote these words as a reminder that our systems are so complex, with so many potential vulnerabilities, that even those 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, a hacker infiltrates your organization and destroys data.

When it comes to protecting the reputation of your jurisdiction and your constituent relationships, what matters isn't so much that you've been hacked, but what you do in the aftermath of that incident. Here we examine some suggestions of what you should do in a cybersecurity crisis to help your jurisdiction maintain its reputation—the 'respond' phase of the NIST Cybersecurity Framework.

Rule Number One: Don't Panic

When you discover that your jurisdiction 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 constituents may be aware.

Reassure your staff that you have a business continuity and disaster recovery plan in place and that you have 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 cyberattack, and you intend to do your best to implement them. Then, pull out your crisis management plan (more to come on that).

Rule Number Two: Follow Applicable Laws

Government entities in the state of Florida are subject to the statutes contained within the Florida Information Protection Act (FIPA). Fortunately, 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 constituents 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)

The European Union's General Data Protection Act (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). Federal, state, and local government entities may be subject to its guidelines in certain instances.

Government Technology magazine looked into GDPR's potential effect on state and local governments when the law came into effect, reporting, "Anya Burgess, a spokeswoman with the United Kingdom's Information Commissioner's Office, told Government Technology that GDPR only applies if individuals who receive the product or service reside in Europe. As a result, GDPR does not apply if a U.S. government agency collects PII data on a citizen of Europe who is visiting or living in the U.S. and uses that government agency's services or products while in the U.S." ("Will GDPR Rules Impact States and Localities?" *Government Technology,* May 3, 2018.)

The article did point out one potential area of concern, especially relevant for Florida, which is tourism advertising. Speaking with Dirk Hensel, a spokesman for Germany's federal commissioner for Data Protection and Freedom of Information, the magazine reports, "...if the state of Florida's tourism department, for example, launches a promotional campaign to target residents living in Europe to come visit the Sunshine State, then any PII data collected on those German citizens by the state of Florida would likely fall under GDPR requirements...." ("Will GDPR Rules Impact States and Localities?" *Government Technology*, May 3, 2018.)

If you need help or further guidance, you should consider consulting a GDPR expert. You can learn more at the EU's official GDPR website, 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 that you have a best practice plan, that you are working hard to limit the damage, and that law enforcement authorities have been notified. Amid crisis, it is vital that a government entity is seen as calm-headed, professional, and forthright.

Many experts recommend as much transparency as possible 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: Many security teams add a simply written notification FAQ to any cyberattack or breach notification they announce publicly, and it's typically seen as helpful. A plain-English FAQ is helpful because your citizens may not be lawyers or technically minded, and they likely will appreciate being able to quickly read clear answers to their 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 any 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 guide how transparent you can be and how and when to provide updates to your staff and constituents.

The Devil Is in the Details: Some teams like to be very specific when they talk about the method of attack and point of entry, but others are deliberately vague with their language, and that can become frustrating to constituents. Sometimes you may not be able to talk about the details, especially if you are working with law enforcement, as noted earlier. In general, it is important to be as specific as you can with your constituents 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, the general public appreciates it when organizations accept responsibility. One way to begin rebuilding trust with your constituents is to let those affected see you take ownership of the crisis and act responsibly in the aftermath.

Preparing for Crisis Before It Happens

When a cyberattack happens, 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, 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 establish strategies and procedures that your staff can implement before, during, and after a cybersecurity crisis to prevent a cyber incident from growing into a full-blown crisis.

FROM THE SURVEY

35% of respondents have cyber insurance.

To be ready for a cyberattack when it happens, consider building an internal crisis management team so that you are ready as a unit and make sure that the necessary resources are ready in advance.

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 leaders see cyber incidents as an IT issue, with the IT department being the only group involved. But more effective crisis plans typically involve a coordinated response from multiple departments (operations, compliance, regulatory/legal, public relations, HR and finance) and draws upon skill sets from across your organization when a cybersecurity incident occurs, especially when a cybersecurity incident threatens to escalate to crisis level.

Develop a crisis management plan: Your crisis management team should have a cyber-crisis playbook outlining 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 website defacement, theft of hardware, a ransomware attack, and a DDoS attack. Determine who will be responsible for what, such as notifying law enforcement and public outreach. Who will speak for the organization and what will the messaging be? It's best to have a template in place before an actual crisis.

This cyber planning is important because it can help prepare your organization to respond to specific threats and informs your staff about potential ways to handle cyber incidents, hopefully, to limit the damage to your organization. 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 important to rehearse these training steps and other associated activities regularly, using live drills to make sure that your crisis management team is practiced in delivering a smooth and effective response when crisis calls.

Cyber Insurance

With increasing stories of government organizations falling victim to cyberattacks and high-profile ransomware infections, 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.

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. Because payouts are often capped, premiums are typically expensive, and cyber insurance is not generally a comprehensive solution, it may not be cost-effective enough for may government entities to consider. But, considering the potential impact on the citizens in your jurisdiction, cyber insurance may be a prudent investment. Just don't make the mistake of thinking that it replaces employee cybersecurity training and good cybersecurity planning.

WHEN TO CONSIDER CYBER INSURANCE?

Government organizations typically store and process many types of personally identifiable information like health records and financial information on customers and online account information, such as security answers and questions, passwords, and email addresses. Compared to business entities, governments typically handle highly curated personal information such as tax, voting, public

health, and licensure information. The value of this information is considerable, and the cost of a breach high.

As with any other kind of insurance policy, the idea of 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 a government entity does experience a data breach, then your cyber insurance company can act as a crisis management partner as your policy may include incident response as a form of coverage. Cyber insurance can help minimize the financial impact on your budget allocations and provide consumer protections to those individuals and organizations affected by the breach.

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.

Agency Impersonation

Due to the trusted position government entities hold and the fact that nearly everyone has some connection to a government body (such as possessing a driver's license or paying taxes), government entities are often impersonated for fraudulent activity. As mentioned earlier, hackers regularly impersonate the U.S. Internal Revenue Service in phishing emails to taxpayers, accountants, and payroll personal in an attempt to gather PII. Local governments that administer utilities and services for their citizens may also be targets for impersonation.

To help prevent fraud by impersonation, do not send emails or text messages to your citizens that contain links or attachments. Inform your citizenry that your jurisdiction will never send emails containing links or attachments and will only request that citizens log in to their accounts on their own to take action. Implementing a protocol such as this in your jurisdiction can help ensure that your constituents do not fall prey to email impersonation.

If you become aware that someone is impersonating a department within your jurisdiction, contact law enforcement and notify your constituents as soon as possible. Announce the scam on your jurisdiction's social media accounts and send emails, and perhaps letters, warning citizens to be wary of emails or texts that claim to be from your jurisdiction.

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

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

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 spear-phishing 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 senior leadership. 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.

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 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 senior leadership, 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 spear-phishing 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 coworker 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 spear-phishing 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 Skill Set

These are all examples of a cybersecurity culture that is decidedly *unsecure*. 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 spear-phishing 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 spear-phishing 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.

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 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 Senior Leadership 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 senior leadership'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.

Small Changes Make a Big Difference

Mark Clancy, Cyber Florida Board Member and VP & CISO, Sprint

Electronic mail is one of the ways organizations 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 (BEC), and the FBI estimates that in the last 5 years, BEC has cost organizations over $12 billion dollars in losses. No organization 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 is 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 organization. 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.

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.

What can I do to make my organization 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]

[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/*

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 organization'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 organizational 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 organization'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 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/gov 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.

WiFi 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 WiFi network, make sure it is secure and hidden. To hide your WiFi 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 WiFi 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, easy-to-guess passwords such as 'password,' '123456,' 'qwerty,' etc.
- Select four or five seemingly random words that are easy for you to remember, but difficult for others to guess and sprinkle numbers and symbols in when possible, such as 'pepper0nipizzais100%lit.'

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

CYBER FLORIDA

at the UNIVERSITY OF SOUTH FLORIDA

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