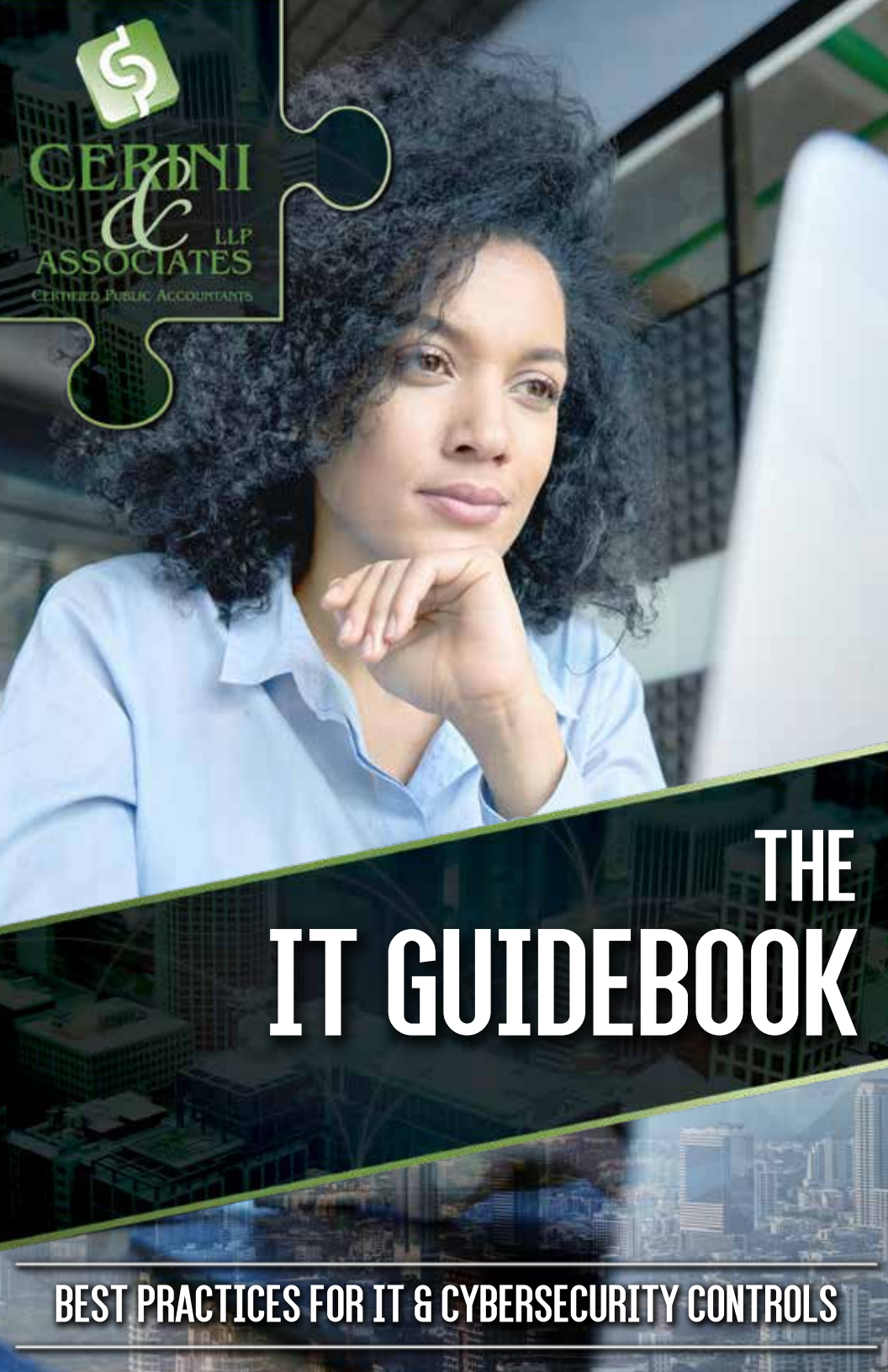

CERINI & ASSOCIATES LLP
CERTIFIED PUBLIC ACCOUNTANTS
THE
IT GUIDEBOOK
BEST PRACTICES FOR IT & CYBERSECURITY CONTROLS

FROM THE EDITOR - SHARI DIAMOND, CIA

They say it takes a village to raise a child. With cybercrime rising, it takes a coordinated effort to stay ahead of the threats. Cybercrimes are getting more sophisticated, criminals more creative, and COVID has made the world more susceptible now that remoting and hybrid working is the new norm.

As you will see in this guidebook, maintaining a strong cybersecurity environment is not just the responsibility of the IT department. This guidebook contains articles that discuss different aspects of the IT environment and is a collaboration among various leaders in the field. Take the time to read through this guide and use this to start a dialogue with your IT department or outsourced IT company to ensure your IT environment is protected and you are well prepared for an unfortunate event. If you have any questions about any of the materials within this guide, please reach out! Don't bury your head in the sand! Our contact info, along with the organizations who partnered to create this guidebook, is below.

CONTRIBUTORS

WRITERS

KEVIN URSO
PRESIDENT
CONNECTED TECHNOLOGY
(631) 724-6504
KURSO@CONNECTEDTECHNOLOGY.COM

JIM DORAN
AREA VICE PRESIDENT
GALLAGHER
(516) 622-2468
JIM_DORAN@AJG.COM

STEPHEN BREIDENBACH
ASSISTANT GENERAL COUNSEL - TECHNOLOGY
MORITT HOCK & HAMROFF, LLP
(516) 873-2000
SBREIDENBACH@MORITTHOCK.COM

LISA M. DEMARCO
VCMO
PUPFISH SUSTAINABILITY SOLUTIONS
(631) 403-1100
LDEMARCO@PUPFISHUSA.COM

JOSHUA PESKAY
VCIO / CYBERSECURITY
ROUNDTABLE TECHNOLOGY
(207) 370-4647
JOSHUA@ROUNDTABLETECHNOLOGY.COM

JOSEPH HOROWITZ
DIRECTOR OF COMPLIANCE AND AUDIT
STETSON CYBERGROUP
(631) 417-3726
JHOROWITZ@STETSONCG.COM

EDITOR

SHARI DIAMOND, CIA
PARTNER
CERINI & ASSOCIATES, LLP
(631) 868-1143
SDIAMOND@CERINICPA.COM

ASSOCIATE EDITOR

KEN CERINI, CPA, CFP, FABFA
MANAGING PARTNER
CERINI & ASSOCIATES, LLP
(631) 868-1103
KCERINI@CERINICPA.COM

PAGE LAYOUT & DESIGN

KRISTINA LAINO-TORTORICE
GRAPHIC DESIGNER
CERINI & ASSOCIATES, LLP
(631) 868-1148
KLAINO@CERINICPA.COM

CONTENTS

INTRODUCTION

March 2020 forced companies to quickly change as the world grappled with the pandemic. So, *what should your priorities be?* Your business goals, simply stated, are:

1. *to make a profit (if you are an owner or have stockholders),*
2. *provide valuable products and services to your customers and/or stakeholders,*
3. *remain competitive and finally*
4. *stay in business. You can't do the first three if you aren't in the game.*

The best ways to stay in business are to:

1. *manage your finances,*
2. *plan for future growth reacting to market trends, and finally*
3. *stay out of trouble.*

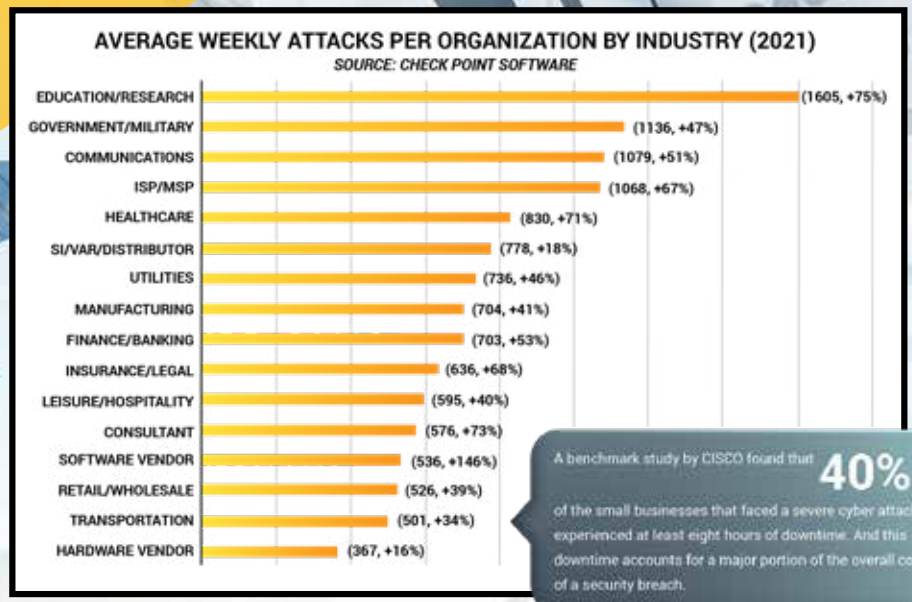
This guide will hit on all three of these points. In summary, you need IT systems you can rely on in order to make the right decisions about the first two points. How to stay out of trouble involves remaining compliant with all laws and regulations, staying on top of threats, and continually implementing security measures. Keep yourself from being in the news as one of the breach statistics. The best way to stay out of the news is to protect your systems, personnel, customers, intellectual property, and brand reputation from cyber criminals. Good news is that the basic control concepts haven't changed: *it's how you are implementing the controls and how honest you are about your adherence and commitment to a strong IT control environment.* Ask yourself:

- *Do you truly understand the threats and risks that are out there?*
- *Do you have sufficient resources both financial and staffing to address and mitigate those risks?*
- *Have you communicated the risks to management and more important, are they listening?*

Yes, there are a lot of components to digest. Start at the beginning by first understanding the risks and the best practices for implementing IT controls.

CYBERSECURITY RISKS

Cybersecurity risks have grown exponentially in the past decade's. Every company that has data is at risk of having that data exposed to hackers: social security numbers, credit card numbers, medical records, driver's license numbers, bank accounts, financial reports, investment records, proprietary software code, trade secrets… *you get the point.* While dumpster diving is still a means to get at data, hackers now have multiple platforms to get into your system. Their goal is to extort companies who do not wish that data to be in the hands of the public. Let's get into some recent statistics to help understand the risks and threats facing all businesses.



A benchmark study by CISCO found that **40%** of the small businesses that faced a severe cyber attack experienced at least eight hours of downtime. And this downtime accounts for a major portion of the overall cost of a security breach.

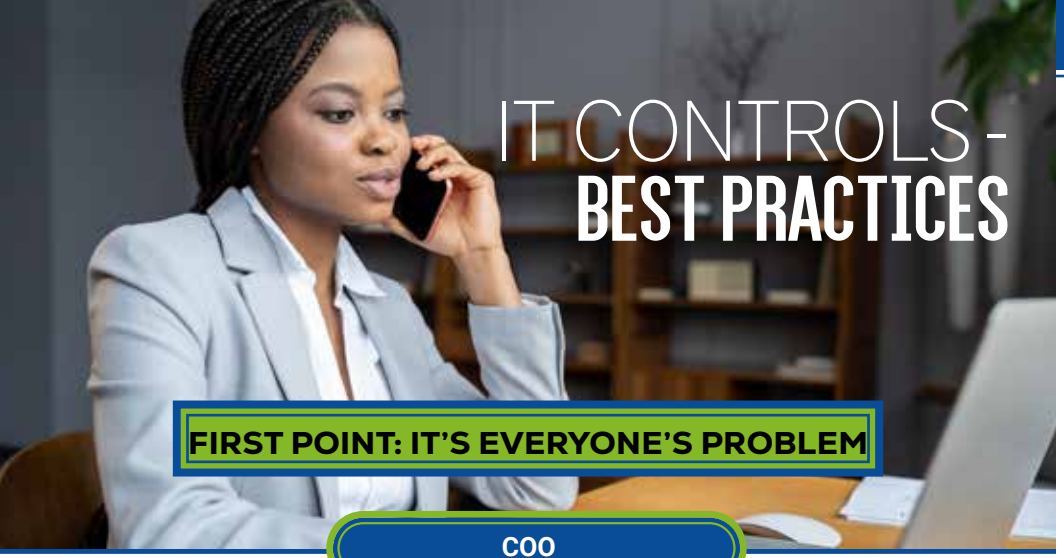
43% of cyberattacks target small businesses (Cyberint)

The above-mentioned CISCO study also found that ransomware was not among the top three cyber threats identified by small businesses. Business owners may be underestimating the threat of ransomware, however, MSPs are not.

85% of MSPs consider ransomware one of the biggest threats to their SMB clients.

95% of cybersecurity breaches are a result of human error (Cyberint)

83% of small and medium-sized businesses are not financially prepared to recover from a cyber attack.



IT CONTROLS - BEST PRACTICES

FIRST POINT: IT'S EVERYONE'S PROBLEM

COO

Ultimately responsible for the operational viability of the firm. The COO must support the CIO and CTO. They must hold every employee to a high standard of protecting the firm's interests through careful attention and vigilance in upholding the employee code of conduct as it relates to IT Controls. There should be consequences for any lapses. This is a serious matter. The COO is responsible for working with the CFO to get appropriate funding for IT Controls solutions. The COO should also work with legal firms and insurance companies with expertise in IT Security to better understand the impacts to an exposure event.

CIO

Responsible for identifying the information needs and identifying critical data required to support decision making within the firm. Also responsible for identifying **PII (Personally Identifiable Information)** and confidential information which could expose the firm and brand and result in public media, personnel, and regulatory compliance consequences. These consequences could be so grave as to cause the company to cease being viable. Not properly identifying this information and not taking direct and appropriate action to mitigate risks is unacceptable given the current cybercrime landscape and could even be considered criminally negligent.

CTO

Responsible for protecting the critical information identified by the CIO through IT security controls implementation and related training. Every effort should be made to automate controls, but training will also be necessary to decrease vulnerability from social engineering attacks.

EMPLOYEES AND VENDORS (*INCLUDES CONSULTANTS*)

Responsible for following the Employee Code of Conduct as it relates to IT Controls and Security Training. Employee and vendor breaches must be tracked and failure to comply with controls (*whether intentional or otherwise*) should result in appropriate discipline including termination or legal action. One crack in the foundation is all it takes.

START WITH A PLAN

Assemble a team that is responsible for creating and maintaining a plan to identify business priorities (*aka* ***critical business functions***), identify threats to those priorities and document the impacts of those threats, and develop controls to mitigate those threats. There is a cost to mitigation, so that's why it is very important to understand your specific priorities and their impacts. More money should be applied to the more critical and valuable business functions. Priorities should be re-evaluated on an annual basis and when there is a disrupting event in the economy or industry.

The plan should be supported by the C-team and will be the direct responsibility of the COO, CIO, and CTO (*or equivalents*) of the organization. Use of an Internal Auditor (*in-house or outsourced*) is a great way to kick off this process. Use of outsourced full-service IT firms with specialization in cybersecurity implementation and training are also critical to a successful outcome. That said, it is not easy to find the right resources, but they are out there.

CONTINUED ON NEXT PAGE

DEVELOP A CODE OF CONDUCT (*YOUR IT CONTROLS RESPONSIBILITIES*)

Every employee and vendor should be held to a written set of responsibilities and be required to attest to their understanding and acceptance when they are first hired, annually, and for any consequential updates. Acceptable behavior and unacceptable behavior should be laid out in clear language with behavior, impact and consequences clearly related. Impact and consequences are extremely important to enable the reader to fully internalize the importance and necessity of each concept.

It should not be assumed that an employee or vendor will read and completely understand all of the concepts in the Code of Conduct, even if they agree to the terms. Verification through additional training and testing are required to re-enforce these concepts.

Not every employee and vendor will be responsible for EVERY control. Some controls are only relevant to the specific role that the employee or vendor plays in the organization, so there may be a specific section for each role. For example, someone who does not deal with Compliance for Federal Grants on a daily basis would not need to sign off on that particular section; however, IT Security Control areas like *"Credentials Use," "Internet Use," "Email Use," "Corporate Owned Devices Use,"* etc. would be relevant to all, up to and including the CEO.

In the case of repeated unsatisfactory testing results or a breach of conduct, the event should be recorded and tracked, and the employee and vendor should be provided with remedial education to try to prevent future occurrences. Continuous lack of attention to vigilance will eventually lead to a permanent disposition for that employee or vendor. Limiting the career path or bonus may not be a viable resolution since the employee may become more hostile and become an insider risk to the organization.

IT CONTROLS - BEST PRACTICES - CONTINUED

CLOSE THE HOLES (*YOUR CONTROL BREAK PROCESS*)

Top companies are always looking for risks to their organizations' operations. When they find one, they track it to a satisfactory conclusion as a break in controls; and they take it VERY seriously. Managers are responsible and held accountable for closing all control breaks. All risks are triaged and assigned hard deadlines. There are consequences for managers who do not close control breaks by their deadlines. Since control breaks can indicate a vulnerability, control breaks are held in strict confidence and treated on a need-to-know basis for the resolution team only.

Controls can be technical or non-technical. Here is an example to illustrate how a Control Break Process might work for a technical requirement.

001 Requirement: All Corporate Controlled Laptops must be secured.

001.1 Control: Admin privileges must be removed for all users except the Admin User.

001.1.1 Implementation: <This is the actual procedure that a tech admin would use to remove admin privileges>

001.2 Control: USB ports must be disabled for attaching storage devices.

001.2.1 Implementation: <This is the actual procedure that a tech admin would use to disable USB>

The requirement is the responsibility of the CIO. The control and implementation are the responsibility of the CTO.

A CYBERSECURITY PRIMER

Cybersecurity in a nutshell is the combination of knowledge about what information is valuable in your organization, who wants to exploit it, why they want to exploit it, what your organization is willing to do to prevent a breach of information, and how well your organization responds to a breach event.

WHAT HAPPENS ONCE YOUR ORGANIZATION HAS BEEN COMPROMISED?

After a bad actor exploits your information, it is too late. By that time, the damage is done, and your company is in damage control mode to minimize the impacts. Most people have by now heard of the Dark Web, but what most people don't know is that there is a whole supply chain infrastructure consisting of independent individuals, organized crime syndicates, terrorist organizations, corporations, and governments. They all work together on the web to sell pieces of data they have acquired that are useful to others who will buy them for pennies and assemble all of the pieces for an attack with a big payoff. Pennies add up to dollars especially in third world countries where there are limited opportunities to make a viable living. Many of these criminals are just trying to take care of their families and since they are not involved in the ultimate attack, the ethical and legal impacts become diluted. The fact that this supply chain exists makes it possible for really creative criminals to weaponize the most innocent data for a social engineering attack.

EXAMPLE #1: US DEPARTMENT OF LABOR, JANUARY 2022

The hackers wasted no time starting off the new year with a very persuasive email phishing attack that mimicked the US **Department of Labor (DoL)**. The purpose of the attack was to obtain Office 365 credentials. The hackers spoofed the actual DoL email domain, allowing them to pass through their target's security gateways, and used logo and branding, as well as typical wording, to look legitimate and get the users to think they were invited to bid on a government project. Once users clicked on the attached PDF, users were redirected to the fake site, where the user was requested to enter their Office 365 credentials.

Now you know how easy it is to profit from a security breach and why it is such a growth industry.

WHAT CAN YOUR COMPANY DO TO PREVENT A BREACH?

First, your company can develop a framework as previously described on page 9. Once you have your goals and requirements, you can start to lock down your resources and create hurdles that make it difficult for bad actors to compromise your organization. *Can you prevent a breach?* No, but you can make it very difficult and expensive and therefore unlikely for a bad actor to invest in hacking your company. The old story about running faster than your companion to avoid being eaten by the lion applies here. If your defenses are better than your competitors, the bad actors will be smart and go after your competitors first. Just because a breach may be unavoidable, it is still irresponsible and/or criminal to not take every possible action to protect your organization's livelihood and reputation.

A tightly coordinated plan between your organization and your vendors is critical to build your defenses. Whether your CTO is in-house or outsourced as many are today, especially for smaller organizations, your company needs to identify critical data that your IT Security people will protect. You don't really need to know too much about the technology details as what is in place is likely to change in the near future as Cyber-criminals and their tools and techniques evolve, adapt, and become more subtle and sophisticated. In addition, technology companies are always updating their software, possibly exposing some new attack surface just waiting for a zero day exploit. If there is a vulnerability, it is just a matter of time before someone exploits it. Hopefully it will be found by a user and not by a Cyber-criminal first.

Your IT Security team will take care of securing your resources and keeping your software and systems updated with the most recent security patches, but one of the most common and lucrative ways to exploit your system is through social engineering. This concept of social engineering has been previously described in the example, and some more examples will inform the vigilance required by everyone in your organization.

EXAMPLE #2: RUSSIA TARGET UKRAINE, FEBRUARY 2022

When countries go to war, the attack now can involve much more than the destruction of buildings; through the use of spear phishing campaigns, Russia targeted Ukrainian government agencies, law enforcement, non-government organizations, and non-profit organizations in an attempt to compromise Ukraine's critical support systems.

WHAT ELSE DO YOU NEED TO KNOW BESIDES HAVING A PLAN, WORKING WITH YOUR IT PARTNERS, AND KEEPING VIGILANT?

An essential part of your IT Controls plan should be your basic Business Continuity plan. This is more relevant now than ever. *How often do we read in the news about ransom attacks?* Pretty much daily. If you have a legitimate Business Continuity Plan then you have a much better chance of recovering your data after a ransom attack.

*What is the difference between a **Business Continuity (BC)** plan and a **Disaster Recovery (DR)** plan?* DR refers specifically to recovery from a data disaster. DR usually keeps a snapshot of the data offsite and requires time to restore the data once the primary environment is restored. Business Continuity as the name implies, uses redundant hardware and load balancing across multiple geographically-located data centers to prevent ANY disruption to operations in real time. As such, BC is much more costly than DR. The problem with DR is that no one knows if the backup has been compromised as well until they try to restore it. This is not the case with BC. All cloud environments use BC, which is why many companies have migrated to them.

Recently, some companies that have been able to recover their data from backups have still had their data released to the public if a company failed to pay the ransom. That is a decision your company may still need to make. That is why your overall IT Controls plan should also include an Incident Response Plan. For each potential breach or crisis event (*incident*) scenario, your company should already know who the decision makers and role players will be involved in the resolution process and there should already be a resolution decision tree or script in place. The idea here is that a breach is a stressful and impactful event, so you can lessen the stress and impact by being prepared. With all crises events, the plan should be updated with lessons learned.

5 TIPS FOR CYBERSECURITY - A GUIDE TO PROTECTING YOUR BUSINESS

Small and midsize businesses (SMBs) spend less on cybersecurity than larger organizations. SMBs collect data that cybercriminals want; customer, employee, and vendor names, addresses, social security numbers, dates of birth, driver's licenses, and insurance information. This information is everything a criminal needs to commit identity theft and other cybercrimes. Some reports indicate that 71% of data breaches happen to businesses with less than 100 employees. You don't have to be one of the large companies to get attacked. Employing best practices can help protect your company against cyberattacks and data breaches.

The following are best practices that you can take to minimize the chance of data breaches.

1. PASSWORDS/PASSPHRASES

- Use strong passwords or better yet, use a phrase instead of a word.
  - *Consider using passphrases. When possible, use a phrase such as "I went to Lincoln Middle School in 2004" and use the initial of each word like this: "Iw2LMSi#2004"*
  - *Make the password at least 10 characters long. The longer the better: longer passwords are harder for thieves to crack.*
  - *Include numbers, capital letters and symbols.*
  - *Don't use dictionary words. If it's in the dictionary, there is a chance someone will guess it. There's even software that criminals use that can guess words used in dictionaries.*
  - *Change passwords. Passwords should be changed every 60 to 90 days especially if you are not able to implement multi-factor authentication.*
- Don't post it in plain sight. This might seem obvious, but studies have found that a lot of people post their password on their monitor with a sticky note.
- Consider using a password manager. Programs or Web services let you create a different very strong password for each of your accounts, but you only have to remember the one password to access the program or secure site that stores your passwords for you.
- Consider using multi-factor authentication. Set up multi-factor authentication that requires a code that is displayed on your phone. This way hackers cannot access an account without having physical access to your phone.

2. EMPLOYEE SECURITY TRAINING

95% of data breaches are caused by employee mistakes. It is critical to ensure that employees understand the risks to sensitive information and the threat of data breaches. Phishing and ransomware are leading methods of attacks. Employees need to know how to spot phishing emails, phishing websites, and the dangers of email attachments. Training needs to take into account the dangers of hacking, stolen mobile devices, posting sensitive information on social media, and other causes of data breaches. A good training program will continually remind employees about the dangers of data breaches and how to avoid becoming a victim. Cybercriminals are developing new scams and attacks everyday and employees should be made aware of these scams.

3. ENCRYPT DATA

Lost laptops, smartphones, and USB drives continue to cause data breaches. Many businesses don't realize how much sensitive information is on mobile devices. Sensitive information could be in emails, spreadsheets, documents, PDF files, and scanned images. The best way to protect sensitive information is to use encryption. Under many federal and state regulations, encryption is a *"safe harbor."* This means if a mobile device is lost or stolen and the data is encrypted, then the incident would not result in a reportable breach. Customers and affected individuals would not need to be notified.

Types of encryption:

- **Mobile device encryption.** Laptops, smartphones, and USB drives can all be encrypted. This will protect any data that is on these devices.
- **Email encryption.** Emails could contain sensitive information and should be encrypted. Secure email will protect the data that is sent.
- **Workstation encryption.** Like laptop encryption, desktops and workstations can be encrypted to protect any data stored on them. Workstation encryption is very important in the event of a break-in and theft of workstations. Without encryption, a stolen workstation may result in a data breach.

4. DATA BACKUP AND DISASTER RECOVERY

Backing up data will protect your business from data loss due to damaged servers or malicious code such as ransomware. A fire, flood, explosion, or natural disaster can destroy systems that contain valuable information. Having up-to-date data backups and a disaster recovery plan will help recover and restore valuable information. Many businesses go out of business after a data breach because they can't continue to operate without having access to customer information, business process documents, financials, and other necessary information. Data backups ensure that data is recoverable. It is recommended that automated backups occur that securely copy data offsite. Data backups should be tested often to ensure the data is able to be recovered.

5. PERFORM A SECURITY RISK ASSESSMENT

A **security risk assessment (SRA)** is a critical step to understanding the risk to your business and sensitive information. An SRA will inventory customer, employee, vendor, and sensitive data, identify how you are currently protecting the data, and make recommendations on how to lower the risk to the data. Many organizations do not truly understand what data is critical to the organization, what kind of data it is (*e.g., confidential*), how it is being protected, or what the risks are of not protecting the data. An SRA will help you to understand your risk of phishing scams and ransomware, the dangers of lost mobile devices, the risk of insider threats, and how prepared you are in the event of a disaster. Without a thorough understanding of risk, it is difficult to implement the safeguards needed to protect your business. Cybersecurity is a business risk and needs to be evaluated and mitigated just like other business risks.

CONNECTED TECHNOLOGY

OUTSOURCING IT SERVICES AS PART OF YOUR CYBERSECURITY MODEL

Most outsourced IT support companies can provide multiple services thereby allowing a company to focus on its business. It is important to understand what your outsourced IT company is or is not providing, especially with respect to security monitoring, threat detection, incident response, and business continuity and backup. Before hiring an outside contractor or company to provide IT services, you should first determine how much information you are comfortable providing to the IT resource. By outsourcing your information technology tasks, you are hiring third-party contractors or companies to perform the IT work as opposed to having the IT tasks done in-office. Many IT services require that you provide sensitive information pertaining to your business's security and data, so you should also get a clear idea of how the IT resource will protect your information. You may also find that you lose a portion or much of the operational control your company has over certain business functions. Before outsourcing, it's important to determine how much control and governance you want to maintain regarding the operations you will be outsourcing and then make this clear with the company or contractor you hire. You should get this in writing and regularly make sure that the IT support company is upholding its promise. This ensures that your expectations, as well as the responsibilities and roles that you expect from the IT resource, are understood.

MANAGED SERVICES:

If you're spending your time trying to fix IT issues, then you're not concentrating on growing your business, meeting your goals, and keeping your customers happy. Your outsourced IT vendor may have different service levels that can be provided, which can include monitoring, troubleshooting, as well as working with other vendors such as printer companies and internet providers. Managed services should include 24/7 year-round monitoring, patch management, managed enterprise anti-virus, managed malware protection, endpoint security policies, remote help desk, and define service level agreements.

CYBERSECURITY MONITORING AND MITIGATION:

Protecting your business and your employees is no longer an option. The requires ensuring data is properly backed up, disaster recovery and business continuity plans are in place, networks are kept secure to reduce the threat from hackers, viruses, and malware. Many businesses are subject to various regulatory requirements such as HIPAA and your outsourced provider should be ensuring your network operations meet those regulations. Implementing a comprehensive, proactive, 360-degree approach to your IT operations can include:

√ Risk Detection	√ Simulated Phishing
√ Dark Web Monitoring	√ Written Security Policies
√ SPAM/Threat Filtering	√ Disaster Recovery
√ Cyber Awareness Training	√ Networking Monitoring
√ Multi-Factor Authentication	√ Secure Remote Access

BUSINESS CONTINUITY & BACKUP:

Businesses need to be able to recover data quickly in the event of a disaster to keep downtime to an absolute minimum. This requires a data backup solution and a comprehensive business continuity plan that uses state-of-the-art software and robust infrastructure to provide your business with an enterprise-class online computer backup service that ensures you can access files quickly and can get you up and running quickly after any type of service outage. In the past, many backup and recovery plans focused on natural disasters. With ransomware on the rise, backups have helped companies recover their business-critical information allowing their business to continue to operate and avoid paying to get their data back. The pandemic though presented businesses with new challenges with business continuity such as the ability of employees to work remotely, and the ability of businesses to obtain computer equipment due to supply-chain issues.

CLOUD SERVICE:

Recent cyber-attacks have been able to happen due to outdated servers that are hosted on premises. Cloud technology allows you to transfer the physical aspects of your IT, along with their management and maintenance, such that they are delivered electronically through the internet, and charged on a pay-as-you-go pricing structure. Comprehensive solutions allow you to harness the very best of the cloud in order to enhance communication, collaboration and productivity right across your business. Such service can include Office 365, Hosted Exchange, Hosted VoIP, and Secure File Sharing

Keeping up with the ever-changing cyber threats is a full-time job. Because of the complexities and costs of cybersecurity management, many choose to use external specialists with a proven track record in the field — either as a fully outsourced function or in a hybrid model. This can be accomplished by ensuring your outsourced IT company is properly managing your cybersecurity protocols. Many outsourced IT service providers have a team of technical staff who are experienced in the various threats as they are consistently working with other businesses. Their staff have the necessary qualifications and certifications who fully understand the security solutions enabling them to implement the right software products so that they can monitor your security. This is critical to ensure your company can operate.

CONNECTED TECHNOLOGY

CYBERSECURITY AUDITS AND ASSESSMENTS

How do you tell if your information technology environment is properly implemented? An audit is the best way to find out. Many organizations do not have sufficient staff or resources to be able to perform such an audit. Even if you do have a robust internal IT department, an independent assessment should be performed. You can't audit yourself. An overall assessment of an organization's cybersecurity practices and controls, both physical and non-physical, is needed to identify areas that can potentially result in unauthorized access and/or confidential and critical data being compromised. A complete cybersecurity audit entails assessing risks, reviewing policies, reviewing documented controls, assessing compliance with regulations, and providing recommendations to strengthen the internal controls.

CYBERSECURITY RISK ASSESSMENTS:

Risk, measured in terms of impact and likelihood, is the possibility of an event occurring that will have negative impact on the achievement of objectives. A Risk Assessment is a systematic process for identifying, evaluating, and prioritizing risks and threats, whether internal or external, facing your organization. The assessment should be based on the **National Institute of Science and Technology's (NIST)** cybersecurity framework, and the **Center for Internet Security 18 (CIS18)** cybersecurity control categories, to identify threats that could affect the confidentiality, integrity, and availability of systems and data and the safety of the people, connected devices, and the physical environment. A Gap Analysis will provide management with an assessment of an organization's cybersecurity policies, procedures, and controls, and their operating effectiveness as well as identifying the gaps required to be remediated to achieve compliance with regulatory requirements. Overall, when complete, each organization will get a better understanding of the capabilities of defenses required to protect against malicious attacks.

REGULATORY COMPLIANCE AUDITS:

A regulatory compliance audit is an independent evaluation to ensure that an organization is following external laws, rules, and regulations or internal guidelines, such as corporate bylaws, controls, and policies and procedures. Compliance audits may determine if an organization is conforming to an agreement, such as when an entity accepts government or other funding. Compliance audits may also review IT and other security issues, compliance with HR laws, quality management systems, and other areas. The compliance audit should assess the overall effectiveness of your organization's compliance practices and protocols with cybersecurity regulations such as HIPAA, PCI-DSS, NYS Ed Law 2d and FERPA, and NYSDFS 23 NYCRR 500.

POLICY REVIEW AND DOCUMENTATION:

A policy is a system of guidelines, implemented as a procedure or protocol, to guide decisions and achieve rational outcomes throughout an organization. The review should assess the current inventory of policies for existence, completeness, and accuracy in alignment with best practices or regulatory requirements and should provide recommendations in updating or initially documenting policies to meet all applicable regulatory requirements.

INFORMATION TECHNOLOGY APPLICATION CONTROLS (ITAC) AUDITS:

ITACs are responsible for protecting the transactions and data associated with a specific software application, are unique to each application, focus on input, processing, and output functions, ensure the completeness and accuracy of records created by the application, the validity of data entered into those records, and the integrity of data throughout the lifecycle. ITAC audits, or information systems audits, examine the management controls IT infrastructure and business applications. ITAC audits can be performed as a stand-alone assessment or in conjunction with internal audit, or other form of attestation engagement.

INFORMATION TECHNOLOGY GENERAL CONTROLS (ITGC) AUDITS:

ITGCs apply to all systems, components, processes, and data for a given organization or **information technology (IT)** environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations. As part of an ITGC audit, an assessment your organization's controls related to logical access over infrastructure, applications and data, system development life cycle, program change management, data center physical security, system and data backup and recovery, and computer operations should be performed.

DEPARTMENT OF DEFENSE (DOD) AND CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC):

To safeguard sensitive national security information, the **Department of Defense (DoD)** launched the **Cybersecurity Maturity Model Certification (CMMC) 2.0**, which replaced NIST 800-171 on DoD requirements in late 2020. This is a comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks. The CMMC will not allow for self-attestation, and every organization that does business with the DoD will be required to undergo an audit by an authorized auditing entity before bidding on a contract or subcontracting to a prime. By assessing your current policies, procedures, and controls, an assessment can provide recommendations and work with organizations to achieve CMMC compliance.

SOC 2 TYPE 2 READINESS:

A SOC 2 Type 2 report is an internal controls report capturing how a company safeguards customer data and how well those controls are operating. Companies that use cloud service providers use SOC 2 reports to assess and address the risks associated with third party technology services. An assessment can be performed of your current policies, procedures, and controls to achieve SOC 2 Type 2 audit readiness.

VULNERABILITY ASSESSMENTS AND PENETRATION TESTS

There is some confusion between what a vulnerability assessment accomplishes versus a penetration test. While both are critical in reducing cybersecurity attacks, a vulnerability assessment encompasses scanning the environment for anomalies within your IT environment. There are several software products that can be used to scan the environment and report on when changes have occurred and highlight those events that warrant further investigation, and scans should be performed regularly to ensure the environment is secured. When new equipment is deployed or changes in equipment occur, a vulnerability scan should be performed. It is a good practice to establish a baseline of key equipment to facilitate the review if there are any changes and to quickly identify any unauthorized changes. The scans can report on issues such as missing patches, and outdated protocols. Some organizations do not have the staffing to adequately monitor the scan reports and should consider having their outsourced IT provider perform this or contract with a cybersecurity company.

Penetration testing, also known as pen testing, security pen testing, and security testing, is a form of ethical hacking and requires expertise. It describes the intentional launching of simulated cyberattacks by *"white hat"* penetration testers using strategies and tools designed to access or exploit computer systems, networks, websites, and applications. Although the main objective of pen testing is to identify exploitable issues so that effective security controls can be implemented, security professionals can also use penetration testing techniques, along with specialized testing tools, to test the robustness of an organization's security policies, its regulatory compliance, its employees' security awareness, and the organization's ability to identify and respond to security issues and incidents such as unauthorized access, as they occur.

As a simulated cyberattack, ethical hacking techniques help security professionals evaluate the effectiveness of information security measures within their organizations. The pen test attempts to pierce the armor of an organization's cyber defenses, checking for exploitable vulnerabilities in networks, web apps, and user security. The objective is to find weaknesses in systems before attackers do. The results of the pen test can identify where you need more or better controls for monitoring, detecting and responding.

There are different types of pen test strategies that can be implemented depending on what aspect of the technology environment is being assessed and the reason why the pen testing is being done.

WEB APPLICATION PEN TESTING:

Web Application testing is essential to ensure your front-facing systems are protected. The test evaluates the security of a web application with Penetration Testing Execution Standards and, should use the OWASP standard testing checklist. Web application testing will check for application technology weaknesses, technical flaws, or other vulnerabilities, and should also test for any account takeover privileges through host header attacks.

Upon completion, a comprehensive report should be provided on the results and include recommended remediation actions where needed. Variations of pen tests can include:

- blind testing, in which the tester tries to simulate an attack without knowing much about the organization and only using publicly available information (*i.e., domain name, company website, etc.*) to target the organization.
- double blind testing, where only a few people in the organization know that a test will be occurring and can then assess how effective the organization's security monitoring, escalation procedures, and incident and response protocols are working.
- target testing, which involves both the IT and testing teams work together to assess security vulnerabilities as well as incident and response protocols. This is also known as the *"lights-turned-on"* test.

EXTERNAL PEN TESTING:

An external pen test involves performing a dynamic analysis of the organization's network perimeter for any potential vulnerabilities, which may result from an inadequate or improper configuration, known and unknown software/hardware flaws, or operational weaknesses in processes and technical countermeasures. The analysis is carried out from the position of an advisory/hacker and involves active exploitation of vulnerabilities where the testing team attempts to compromise external and internal assets. All technology vulnerabilities should be analyzed against known CVE's. Upon completion, a comprehensive report should be provided on the results and include recommended remediation actions where needed.

INTERNAL PEN TESTING:

Over seventy percent of attacks occur from inside the network. This number continues to grow with espionage, rogue employees, and social engineering at a high. The goal of an internal pen test is to determine the potential impact a security breach can have on your organization and validating how easy an attacker can maneuver or escalate your environment to overcome your security infrastructure. This is performed from within the organization. Upon completion, a comprehensive report should be provided on the results and include recommended remediation actions where needed.

STETSON cybergroup

INCIDENT RESPONSE PLANNING

IMAGINE THIS:

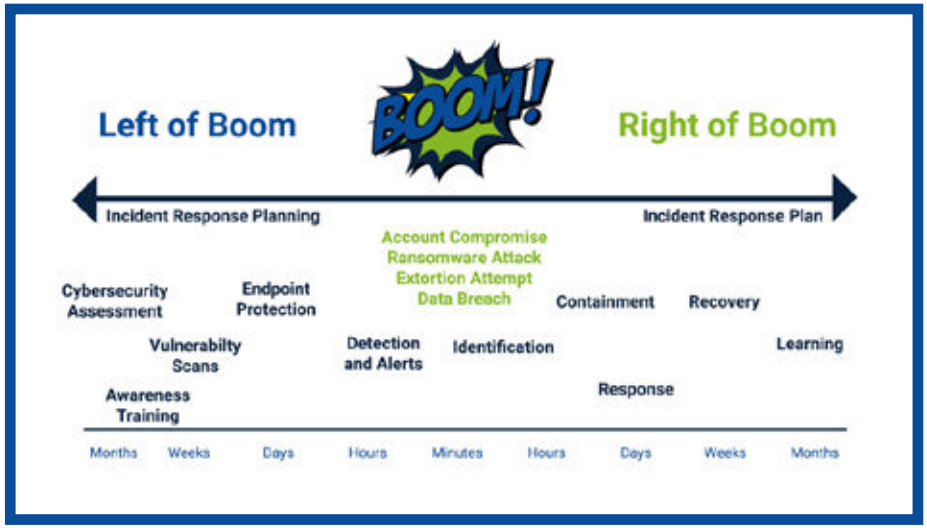
You're the Executive Director of a $5 million dollar nonprofit organization. It's 6:30 AM on Monday morning and even though you wish you were still sleeping; you are logging into your email to follow-up with some donors. You get a login error message, wrong password. You're still waking up, you probably typed it wrong. You take a sip of coffee and type in your password again. **Wrong again.** Another sip, another try. **OK:** *now you are **SURE** you are using the right password.* You pick up your phone and as soon as you unlock it you see that you have a bunch of unread text messages. Your phone starts ringing - it's your trusted and incredibly competent office manager, calling with some bad news: **no one can login** and it appears you are under attack. Hackers apparently want a specific sum of money to unlock your email accounts. This is a nightmare though you are surely awake.

Your brain starts working and you ask if you can *"just call Google and have them reset our accounts or something,"* but there's more bad news: the hackers reveal they have personal information of all your donors and will leak it on the dark web if payment is not made. As the Executive Director, you are being asked: *"What's the plan?"*

Was your plan that this wouldn't happen to your organization?

WHAT IS AN INCIDENT RESPONSE PLAN?

In the image below, the ***"BOOM!"*** represents the incident itself. It could be any type of cyber incident, including the one we just described, but it could also be a natural disaster like a hurricane or flood, a terrorist attack, a sudden death or absence of key personnel, or any incident that severely impacts your operations. For purposes of THIS article, we are focusing on cyber incidents such as account compromise, data breach, ransomware, and extortion. A company that does not already have a cybersecurity **incident response plan (IRP)** should strongly consider engaging with a consulting firm who has expertise to develop a detailed plan. A consulting company will ensure that there are no critical omissions that could cause the plan to fail during a real live incident. It is always better to plan and be prepared. Remember, if you are locked out of your system, make sure you can still access your IRP which should be stored out-of-band and accessible during an incident response.



*Please note that the items listed left of boom are not meant to be a **comprehensive** list of protections - there could reasonably be dozens of items listed there - we are just listing a few of the major ones.*

CONTINUED ON NEXT PAGE

WHY DO YOU WANT AN INCIDENT RESPONSE PLAN?

Preparing an **incident response plan (IRP)** accomplishes two primary objectives, both of which have tremendous advantages for your organization:

1. In thinking about the types of incidents that may occur and how they will impact you, you will not only be better prepared, but you will identify actions that can reduce the likelihood and severity of those incidents.

2. By having an incident response plan in place, you will be able to reduce the impact of an incident when it does occur.

The case for incident response planning becomes a bit clearer if we remove it from our first image:

THE THREE MOST CRITICAL COMPONENTS OF AN INCIDENT RESPONSE PLAN

1. DECLARATION

An incident response plan must include guidelines for what constitutes an incident and procedures for declaration.

2. IR TEAM AND CONTACT INFORMATION

The IRP must include the names and roles of the incident response team along with contact information for ALL the resources that may be needed. This will include technology resources, of course, but also HR, communications, administration, insurance, law enforcement, legal, and any other resource that may be needed in a response.

3. PROCEDURES

The IRP must include what individual steps should be taken, by whom and in what order. In certain types of incidents (*such as data breaches*) the consequences of failing to follow a procedure can be very costly. For example, if an overzealous technician wipes a computer that was compromised, they might erase forensic evidence that could be critical in filing an insurance claim.

INCIDENT RESPONSE PLANNING - CONTINUED

PHASES OF INCIDENT RESPONSE

The articles linked at the end will each have slightly different phases. Some resources list 4, 5, 6, or more phases. For brevity's sake, let's go with four **(4)** here, but use whatever works best for your organization in your plan.

1. DECLARATION:

The declaration phase occurs when an incident is first detected and is determined to satisfy the criteria for invoking the IRP.

2. CONTAINMENT:

The containment phase is usually (*but not always*) performed by technical personnel and involves limiting the impact of the incident as quickly and as safely as possible. It is critically important to follow procedures in this phase to avoid making errors that can increase the liability of the organization and/or destroy forensic evidence.

3. RESPONSE:

The response phase includes all activities involved in responding to and recovering from the incident. Depending on the incident this could include sending out breach notifications, working with incident responders, recovering backups, restoring systems, running scans and tests, and all activities required to restore business operations, constituent confidence, financial stability, and personnel safety.

4. LEARNING:

The final phase, once the dust has settled and everyone has had a chance to take a breath, is to gather the response team and review any lessons learned. There's a famous quote (*sometimes attributed to Winston Churchill and at other times Rahm Emanuel*): *"Never let a crisis go to waste."*

Learning from an incident can be an invaluable experience that can help you be much better prepared in the future. Don't let it go to waste.

HELPFUL RESOURCES

There are many good articles and ebooks where you can learn more about incident response planning. Here are 3 that are highly recommended:

1. (short): Incident Response Plan | Defendify
2. (medium): 6 Phases in the Incident Response Plan | Security Metrics
3. (long): The Incident Responder's Field Guide | Digital Guardian

CYBERSECURITY CONSIDERATIONS FOR SMALL ORGANIZATIONS AND NONPROFITS

Ensuring your organization has a robust cybersecurity environment takes a lot of resources specifically qualified people. For small and nonprofit organizations that don't have the budget to support hiring so many different professionals, this can be problematic. A typical large enterprise will have several C-Suite and other upper management employees overseeing the IT environment and for each of these titles, there are layers of support staff. Think about how banks operate and how many people they have to employ that are dedicated to data governance, privacy, and data protection. That is a luxury that small and nonprofit organizations cannot afford, yet the data they maintain is just as vulnerable to attacks. Small companies often have a small team of maybe one or two people who are given titles like *"System Administrator"* or *"IT Manager"* and may not have the skills to adequately perform any of the IT roles missing from our nonprofit c-suite. Hackers know this and are targeting smaller companies and nonprofits.

Will the person you tasked to manage your small company/nonprofit IT environment know whether the IT resources are working effectively to reduce and manage cybersecurity threats?

Will he/she know what emerging data privacy laws such as GDPR, CCPA, AND NY SHIELD will impact the organization?

Will he/she know whether to renew a big contract for a longtime database vendor or migrate to another cloud-based application?

Will he/she be able to effectively govern?

A lot of questions but there is a solution that can help: using a virtual CIO (*known as a vCIO*). Let's take a deeper look at how this can play out.

In this role, the vCIO meets with the COO regularly and spends time learning about the overall organizational strategy and where the information technology is succeeding or failing in supporting that strategy. The vCIO works with the COO to make sure he/she understands the larger organizational needs and only then begins working with COO on the information technology strategy.

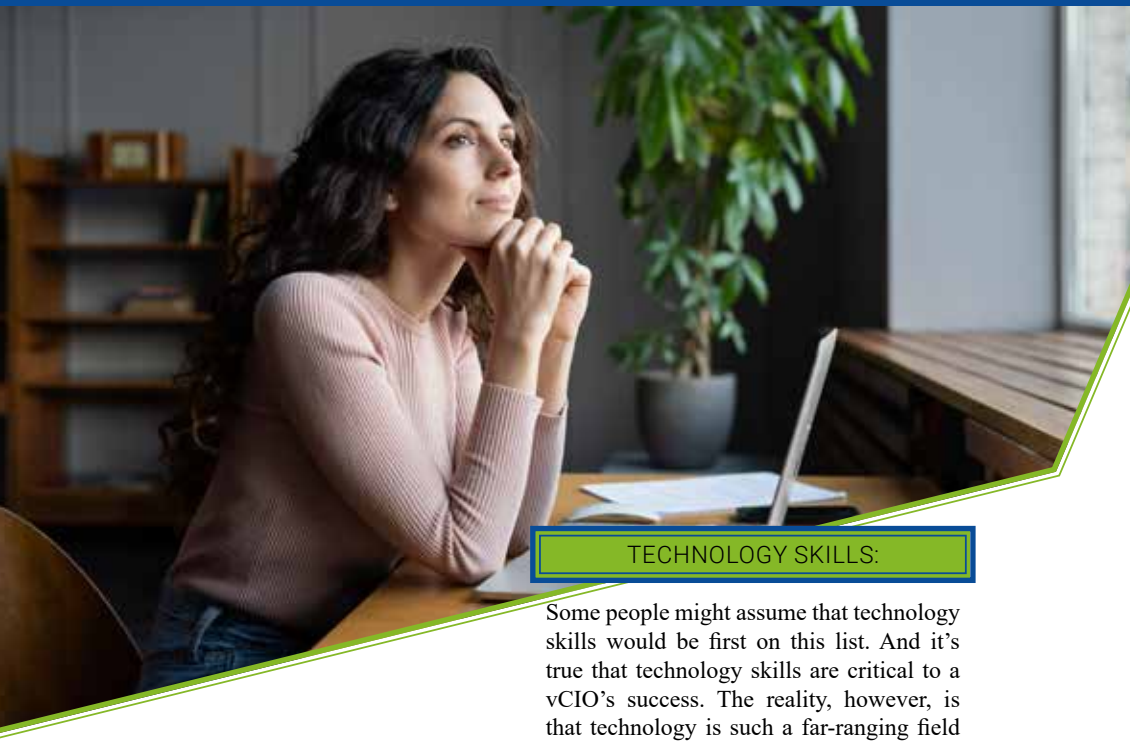
The vCIO meets with the IT staff (*and/or the outsourced vendor(s)*) and establishes appropriate expectations for roles, responsibilities and service delivery; works with the COO to establish key measures of success for IT; helps the COO better understand the current cybersecurity posture, identifies risks and provides recommendations for risk mitigation; and helps clarify what data privacy regulations apply to the organization and helps establish a two-year roadmap toward compliance.

When the COO gets tasked with managing the information technology component of the annual financial audit, the vCIO helps the COO and the team review the prior year's findings and coordinate the gathering and providing of requested documentation to the auditors. The vCIO also sits in on the IT audit meetings and helps the organization respond to audit questions and findings.

After several months of working together, The vCIO and the COO gather a group of senior leaders at the organization and form a technology steering committee. Twice a year, the vCIO and the COO prepare a comprehensive presentation for the steering committee that includes an updated technology roadmap, a strategic technology plan and an executive summary of both completed and planned projects.

The end result is that the COO can better manage and effectively govern technology for the organization through communication from key stakeholders across the organization.

CONTINUED ON NEXT PAGE



WHAT ARE QUALITIES OF AN EFFECTIVE VCIO?

LEADERSHIP SAVVY:

A vCIO needs to work with leadership to understand organizational goals and how information technology can help support those goals. Technology cannot exist for its own sake, a good vCIO must understand how to convey technology risks and opportunities to leadership in a way that is clear and allows leadership to make well-informed decisions about resource allocation, risk tolerance and prioritization.

MANAGEMENT SKILLS:

An effective vCIO must be able to deliver consistently to help lead a team to high performance levels. This requires experience and skills in active listening, root cause analysis, understanding team dynamics and accountability, project management, change management, delegation, and prioritization.

TECHNOLOGY SKILLS:

Some people might assume that technology skills would be first on this list. And it's true that technology skills are critical to a vCIO's success. The reality, however, is that technology is such a far-ranging field that no single person can be expected to have a high level of expertise in ALL the technological aspects required for today's small business or nonprofit operations. An effective vCIO may have specific areas of expertise, but much more important is a BROAD range of competence across multiple technology disciplines including technology infrastructure, cloud services, cybersecurity, data governance, data privacy, project management, Agile methodology, and emerging technologies.

A GOOD NETWORK:

An effective vCIO needs access to a network that includes a wide range of technology professionals that the vCIO can bring in when specific expertise is needed for a specific technology need. Because no one person can reasonably be expert in all areas of technology, the effective vCIO understands and respects the edges of their competency and not only advocates for bringing in appropriate expertise where needed, but can also recommend specific resources with the needed expertise.

CYBERSECURITY CONSIDERATIONS - CONTINUED

INTERPERSONAL AND COMMUNICATION SKILLS:

A vCIO will have to communicate effectively to a wide range of people about many complex technology topics. A vCIO may have to have *"difficult"* conversations with various stakeholders. One day a vCIO may have to speak candidly with a Leadership about discovered risks. Another day the vCIO may have to have a direct conversation with a system administrator about their performance and a lack of preparedness in weekly team meetings. A vCIO will often facilitate conversations and strategic planning discussions between leadership, the technology team, and other stakeholders, all with different perspectives and levels of understanding about technology. The degree to which a vCIO can effectively navigate these conversations will go a long way toward determining their success.

COACHING AND MENTORING:

An effective vCIO must be able to provide appropriate feedback that helps team members grow and evolve as individuals and as a team. The vCIO should identify skills gaps, and direct team members toward appropriate training opportunities to build the skills of the individuals and teams with whom they collaborate.

Without all (*or at least most*) of these qualities, it will be very difficult for a vCIO to achieve success. Take a hard look at your internal management structure to see if a vCIO may be a good fit to improving your cybersecurity environment and allow your organization to grow.

RoundTable

CYBERSECURITY INSURANCE

Times have certainly changed with respect to cybersecurity controls. Regardless of industry or organizational size, companies should expect to see a continued disciplined underwriting approach that remains laser-focused on data security controls, with rates continuing their upward trend. Organizations will need to grapple with more restrictive coverage terms, mandatory sublimits, and exclusionary language specific to certain global and widespread cyber incidents. Capacity questions have not been settled, and exactly how much will be available in the U.S. and global cyber markets in 2022 remains an open question.

Ransomware attacks continued to ravage the bottom lines of both their victims and insurance carriers. During the first six months of 2021, more money was paid in ransom payments than in all of 2020. Increased payment amounts may be due, at least in part, to the fact that hackers now routinely threaten to publicize their victim's most sensitive data if their six and seven figure ransom demands are not met. However, extortion payments are just one piece of the cyber claim. The average downtime from a ransomware attack is 23 days, more than doubling the costs due to business interruptions. And when companies had to switch to remote operations, the costs of a data breach increased.

The cyber insurance market took four deliberate steps to combat increasing loss ratios in an effort to protect its bottom line.

RATE INCREASES:

Cyber premiums increased across the board, regardless of the industry sector or size of the organization. Cyber underwriters are being cautious or even moving away from specific industries, including municipalities, higher education, technology, and manufacturing.

CAPACITY CONSTRICTION:

There were clear indicators that carriers wanted to limit their exposure through limiting capacity. The policy limits offered during prior renewals were routinely cut to half of that amount during the 2021 renewal cycle, both at the primary and excess layer level.

COVERAGE LIMITATIONS:

Many carriers imposed sublimits and coinsurance provisions specific to ransomware claims. This often resulted in limiting coverage to 50% of the policy limit or less. Certain carriers had to add exclusionary language to specific known vulnerabilities; failure to remediate these could lead to a denial of coverage for losses attributed to them. Others revised coverage terms specific to regulatory claims with language that constricted risk transfer for regulatory risk.

GREATER UNDERWRITING SCRUTINY:

Almost all carriers asked for more details around data security control efforts. Not surprisingly, many questions focused on ransomware prevention and mitigation, with several carriers requiring ransomware supplemental applications consisting of dozens of questions to see how well insureds managed the threat.

Based on the past statistics and future predictions, the cybersecurity insurance market is changing.

CONTINUED ON NEXT PAGE

CYBER INSURANCE UNDERWRITERS:

It has become clear that rate increases alone will not be able to solve the current and future cyber market challenges. There is a focus on changing coverage terms, which are trending to restrict coverage for systemic risk, where a single vulnerability may impact a majority of a carrier book of business. Carriers are beginning to address this in their policy forms by imposing sublimits and/or exclusionary language for these global cyber incidents, and it may impair the buyer's ability to transfer cyber risk in the comprehensive way it did in prior years.

REINSURERS:

Expect markets to seek support from outside the traditional rated capacity market via collateralized reinsurance and **Insurance-Linked Securities (ILS)** transactions with the capital markets. This could also take the form of looking to different reinsurance structures and product development. Also expect continued cyber loss modeling tool development as the market pushes for further insights into the far-reaching threats of systemic cyber risk.

CYBER RISK MANAGEMENT VENDORS:

The service providers that help prevent and mitigate the effects of cyber incidents play a role of growing importance and have become a fixture in today's cyber marketplace. Buyers of cyber insurance will need to leverage these services one way or another, and the vendors that can provide efficient and cost-effective solutions for the needs of specific risk profiles will continue to emerge as a necessity.

GOVERNMENT:

Many are watching an increased effort by both the U.S. and international governments to work with and provide insight to the private sector in managing cyber threats, with a particular focus on the ransomware epidemic. Guidance around OFAC compliance, specific to whether or not ransom payments can legally be made, was provided in 2021, with aggressive action in sanctioning at least one cryptocurrency exchange. The private sector may be subject to severe penalties for noncompliance to government-mandated OFAC requirements. Also, law enforcement is to become more proficient at helping victim organizations recover ransom payments to threat actors, using a combination of cryptocurrency experts, computer scientists, blockchain analysts, and crypto-tracers in this effort. Finally, we expect law enforcement to embark on a more aggressive offensive strategy in disrupting **ransomware as a Service (RaaS)** affiliates.

The cybersecurity insurance industry has changed dramatically in the past 3 years and will continue as hackers become more sophisticated. Regulatory risk continues to evolve as privacy laws around the U.S. and international arenas expand. Data subjects, and the regulators that represent them, are more empowered than ever by the California Consumer Privacy Act, the Illinois Biometric Information Privacy Act, Europe's General Data Protection Regulations, and many other rules. These regulations follow a common theme that holds organizations to specific standards as they collect, store, process, and transfer consumer data. In some cases, noncompliance can lead to regulatory investigations, lawsuits, fines, and settlements and may provide a path for plaintiffs to pursue private rights of action.

Because of the highly nuanced nature of the cyber insurance market, it is imperative that your organization is working with an insurance broker who specializes in your particular industry or line of coverage. To effectively manage the underwriting process, it is essential that your cyber insurance company maintains a detailed working knowledge of the latest cyber insurance products and the requirements to qualify for them. Cyber insurance companies also need to balance renewal timelines with required data security control remediation efforts amidst potential budget limitations. Making sure your technology environment is up to speed with respect to reducing cybersecurity threats is paramount. In order to have effective cybersecurity insurance that permits your company to transfer the risk of a breach, companies must implement stronger cybersecurity internal controls.

DISPOSING TECHNOLOGY

WHAT BUSINESSES SHOULD KNOW ABOUT ELECTRONIC DATA DESTRUCTION AND E-RECYCLING TO MAINTAIN DATA COMPLIANCE, AVOID A CATASTROPHIC DATA BREACH, AND PROTECT THE ENVIRONMENT.

IT Asset Disposition (ITAD) is the process of retiring computer equipment and other IT Hardware and electronics your business no longer uses. While this process need not be complex, the key components - *Data Destruction and Electronics Recycling* - must be a top priority, from a mission-critical and data compliance perspective. In fact, every business, regardless of size or industry should have an ITAD strategy which includes a solid data destruction and disposal plan. Not only will having a plan in place help mitigate the risk of a data breach due to improper ITAD practices, but in most cases, will ensure data compliance and may even reduce the rate of your cyber insurance policy.

Businesses of all sizes – *in every industry* – rely more heavily on technology than ever before. As a result, sensitive data is exchanged at lightning speeds, then saved to hard drives located inside the laptops, desktops, tablets, scanners, servers, printers, and mobile devices we use each day. While data-conscious businesses implement security measures to prevent a data compromise when their equipment is in use, they are often unaware of the steps that must be taken once equipment is retired, leaving themselves vulnerable to a catastrophic data breach long after their computer equipment has been retired and replaced. This substantial, potential liability can lay dormant for years until the hard drives and other media devices are properly destroyed.

Contrary to popular belief, deleting, formatting, or damaging (*hammering, drilling, smashing, or submerging*) a hard drive or any other electronic media will not permanently erase or eradicate data, which remains recoverable long after computer equipment is out of sight and mind. To remain compliant with any one of the Federal, State, and Regulatory Laws, your sensitive data must be destroyed according to the strict guidelines set forth by either NIST 800-88, Department of Defense 5220.22-M, and the NAID standard for clearing, purging, and destroying data. Following these standards will not only ensure compliance but will mitigate your company's risk of a data breach associated with improper data disposition practices.

To appreciate the importance of having an ITAD Plan in place, it is helpful to first understand sensitive **Personal Identifying Information (PII)** and your company's obligation to protect it. This is information that, if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual – employees, clients, vendors, etc. In general, it is defined as any information that could be used by criminals to conduct crimes against an individual, including identity theft. Social security numbers, financial, banking, and credit card information, home and email addresses, driver's license and state identification numbers, healthcare insurance and medical records, student information and test scores, payroll information, and income tax records are all examples of SPII that are collected by businesses each day. Federal, State, and Regulatory Compliance laws dictate how this electronic data must be stored, transmitted, processed and you guessed it – *disposed of* – which is why a solid data destruction and disposal plan is critical to your business.

It is important to first understand your obligation to safeguard the sensitive data hiding on your hard drives and other electronic media. Then, you can begin to take steps to mitigate the risk and ensure data compliance, a term which refers to any regulations that a business must follow to ensure the sensitive digital assets it possesses are guarded against loss, theft, and misuse.

CONTINUED ON NEXT PAGE

Three highly effective and inexpensive Data Destruction methods employed by ITAD providers include:

1. MEDIA SANITIZATION:

Often referred to as Wiping a Hard Drive, sanitization meets up to 24 International Standards including the US Department of Defense's DoD 5220.22-M.

2. DEGAUSSING:

Demagnetizing or degaussing a hard drive renders it completely unusable. To accomplish this, a High Definition 5T degausser with patented internal NSA Approved Field Verification is used. Field strength can then be measured in real-time, ensuring your media is being degaussed to NSA standards.

3. HARD DRIVE DESTRUCTION:

A method that utilizes a hard drive destruction machine to physically fold and destroy the device.

When creating an ITAD Plan, choose a NAID certified IT Asset Disposition firm that offers seamless integration by collaborating with your Managed Service Provider, or works as an extension of your own IT Department to develop or execute your strategy. Not only should they offer the Data Destruction options above, but also ensure that chain of custody is maintained, and the data destruction process can be recorded and saved as visual proof with Certificates of Data Destruction, an invaluable asset in the event of an audit.

Sustainable technology practices pertain to the management, repurposing, and lawful disposition of IT hardware in a manner that reduces environmental impact and is the final component of a comprehensive IT/Electronics disposal plan. Obsolete IT assets and other electronics are considered toxic waste and by law must be properly recycled, which conserves natural resources and reduces air and water pollution, as well as greenhouse gas emissions that are caused by manufacturing virgin materials. Equipment that cannot be repurposed should be carefully dismantled to prevent damage to components that may be reintroduced back into the manufacturing stream since electronics are made from valuable resources and materials, which require energy to manufacture. Not only is this a critical process since electronic waste represents 2% of the trash in US landfills but equals 70% of overall toxic waste in the US alone - but prioritizing Sustainable Technology will help your organization reduce its environmental footprint and meet Corporate Social Responsibility goals.

IT Asset Disposition practices are more time-consuming than complex. Having a strategy in place will ensure process and procedure is followed when it is time to dismantle IT equipment - even if employee responsibility shifts significantly mitigating your organizational risk of a Breach After Disposition and ensuring data compliance.

PUPFISH SUSTAINABILITY

CYBERSECURITY -

LEGAL EXPERT ANALYSIS

NAVIGATING THE AMBIGUOUS REQUIREMENT OF *'REASONABLE SECURITY'* MEASURES WHILE PROTECTING PERSONAL INFORMATION.

Over the last couple of years, cybersecurity laws have commonly required that sensitive information be protected through the use of *"reasonable security."* Business owners have likely heard that they are required to protect sensitive information, but may not understand how to specifically go about this. The term *"reasonable security"* often has been left ambiguous and guidance as to what is required for your specific business might be hard to find.

As a starting point, it is important to understand that what constitutes appropriate security safeguards may depend upon the type of information that you collect and the type of business that you operate. For example, if you are a medical professional, or holding information for a medical professional, you may be subject to the **HIPAA Security Rule (HIPAA)** (*which lists specific safeguards for the protection of electronic health information*), and if you are a financial institution, or holding information for a financial institution, you may need to comply with the **Gramm-Leach-Bliley Act (GLBA)** (*which identifies specific requirements and safeguards for the protection of customer information*).

Administrative guidance elaborates on each of these laws by laying out certain cybersecurity safeguards that should be put in place, including but not limited to: *access controls, monitoring solutions, and disaster recovery procedures.* Further, under both HIPAA and GLBA, if any of the regulated entity's vendors receive protected information from that regulated entity, then the regulated entity is required to contractually bind that vendor in writing to treat the protected information in the same manner as the regulated entity.

In addition to laws and regulations that require entities to implement appropriate safeguards, attorneys' ethical requirements provide guidance on determining what constitutes reasonable security and read in the requirements to implement specific cybersecurity safeguards. Even if, however, you are not subject to the laws and regulations referenced above, if you collect private information from a New York state resident, you are still required to implement reasonable security. As of March 21, 2020, the New York **"Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act)** specifically requires that any person or business that collects private information of a New York resident must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information, including but not limited to, disposal of the data.

CONTINUED ON NEXT PAGE

Private information includes:

1. *Social Security numbers;*
2. *driver's license numbers or non-driver identification card numbers;*
3. *account numbers, credit or debit card numbers, if those numbers would permit access to an individual's financial account;*
4. *biometric information; or*
5. *a user name or email address in combination with information that would permit access to an online account.*

The SHIELD Act enumerates several administrative, technical and physical safeguards that larger businesses must develop, implement and maintain. These safeguards include, but are not limited, to: identifying reasonably foreseeable internal and external risks; assessing risks in network and software design, information processing, transmission, storage and disposal; and detecting, preventing and responding to attacks, system failures and intrusions. For small businesses, the Act simply provides that *"the small business' security program [should contain] reasonable administrative, technical, and physical safeguards that are appropriate for the size and complexity of the small business' activities, and the sensitivity of the personal information the small business collects from or about consumers."* A small business is any person or business with fewer than 50 employees, less than $3 million in gross annual revenue in each of the last three fiscal years, or less than five million dollars in year-end total assets.

Despite all of these legal requirements and safeguards, what constitutes *"reasonable security"* remains ambiguous to this day. As previously noted, most laws currently provide that the safeguards implemented by a business should be reasonable and appropriate, given the size of the business and the information they collect. Agencies such as the **Federal Trade Commission (FTC)** have recognized that there is no such thing as perfect security, but that security is a continuing process that requires the business to detect risks and adjust their safeguards accordingly.

While these sources do not provide a ceiling for the safeguards that a business should have in place, they appear to have at least begun the creation of a floor. For years, the FTC has been the primary enforcer of cybersecurity regulations. The FTC has brought numerous actions for deceptive or unfair business practices under the FTC Act for businesses that claimed—*but failed*—to have reasonable security in place.

Consequently, as best practices, businesses seeking to come into compliance are well-advised to draw knowledge from the publications of their regulators and to also consult the FTC's published guidance on what their type of business is required to implement. Many of these FTC guidelines go into greater detail of the types of safeguards businesses should implement, including: FTC's guidelines for small businesses and the FTC's explanatory material on the Cybersecurity Framework published by the **National Institute of Standards and Technology (NIST)** (*a voluntary framework that includes standards, guidelines and best practices to manage cybersecurity risk*).

CYBERSECURITY - LEGAL EXPERT ANALYSIS - CONTINUED

Bear in mind that if you collect information from individuals located in other states, you will also have to evaluate the laws of those states, which may be stricter than the laws of the state in which your company has its principal place of business. For example, unlike the SHIELD Act, the **California Consumer Privacy Act of 2018 (CCPA)** provides a private right of action to California residents whose personal information was subject to *"an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices."* This private right allows a successful plaintiff to recover damages in the amount of *"not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater."* To put this in context by way of example, if a compromised database has information on a mere 10,000 people, a business could be subject to damages of $1,000,000 to $7,500,000. In contrast, New York's SHIELD Act imposes civil penalties of not more than $5,000 for failing to implement reasonable security and, under New York's Breach Notification law, potential penalties are the greater of $5,000 or up to $20 per instance for failing to notify affected consumers of a data breach, not to exceed $250,000.

As most businesses collect and maintain sensitive personal information about their customers, the key takeaway is to first assess the type of business that you operate and the types of personal information that you collect. From that starting point, develop, implement and maintain a sound security plan to collect only the information that you need, to keep that information safe, and to dispose of it securely. This will form the foundation to help your business meet its legal obligations to protect that sensitive data.

Moritt Hock & Hamroff LLP

RECOMMENDED IT POLICIES

Good governance and accountability require an organization to adopt policies and procedures related to IT to provide criteria and guidance for the company's computer-related operations. To effectively protect computing resources and data, companies should have an acceptable use policy to inform users about appropriate and safe use of company computers, a hardware sanitization policy to ensure that equipment is not discarded with sensitive data, and a breach notification policy in the event that sensitive data is compromised. These policies should be reviewed periodically and updated, as necessary, to reflect changes in technology or an organization's computing environment.

Management and the Board are responsible for creating policies and procedures to properly safeguard PII or PPSI against unauthorized access, misuse, or abuse. This includes data that resides on all types of computing devices from laptops to cell phones. Therefore, policies should also define which devices are covered (*e.g., company-owned or personally-owned*), and should indicate the procedures for reporting lost or stolen devices, as well as the process employees must adhere to before connecting a new device(*s*) to the system.

Lastly, all information, whether in printed or electronic form, should be classified by assigning a level of risk to various types of information. The risk level assigned should be based on the criticality of the information and the need for appropriate security protocols. Once classified, the data should be labeled in a consistent manner to ensure data confidentiality, integrity, and availability. This is especially important if there is a data breach due to unauthorized system access or theft of equipment.

The following is a list of sample policies related to IT and their purpose:

ACCEPTABLE USE OF COMPUTER EQUIPMENT AND INTERNET:

Describes how staff can and cannot utilize the School's computer related technology. Defines the IT security protocols, how often passwords should be changed and the complexity of such passwords, what rights employees have within the various systems, the back-up protocols, and recovery testing requirements.

INFORMATION SECURITY BREACH AND NOTIFICATION POLICY:

This policy would detail how an organization would notify an individual(*s*) whose private information was or is reasonably believed to have been compromised.

CYBERSECURITY POLICY FOR REMOTE USERS:

This policy would stipulate guidelines for complying with security protocols when working remotely or when traveling. The policy may include the expected use of approved messaging programs with encryption, such as Signal or WhatsApp, updating and patching computer security schedules, like updating antivirus or anti-malware software, and protocols on remotely wiping devices if lost.

DOCUMENT RETENTION AND DESTRUCTION:

States that the School will adhere to State and/or Federal documentation retention requirements (*the amount of time specific documents should be retained should be documented in the procedures*). The policy should also state that the School will comply with any State/Federal requirements regarding the destruction of records.

DATA CLASSIFICATION AND CONFIDENTIALITY:

Describes what information is considered confidential and defines that the School will ensure such information is not to be shared (*specific procedures should describe how information is to be disseminated and protocols for handling sensitive information*).

ELECTRONIC MAIL AND MONITORING:

Notes that the organization's email system is intended for business use only and describes specific instances of prohibited email usage. In addition, the policy states that management has the right to enter, search and/or monitor emails of any employee without advance notice and as consistent with applicable state and federal laws.

INTERNET USAGE AND MONITORING:

Describes the restrictions of Internet usage by employees including personal communication, purchasing personal items, gambling, and using the Internet for displaying, transmitting and/or downloading sexually explicit content. The policy further states that Internet use will be logged, and that management can investigate such usage.

SOCIAL MEDIA POLICY:

As many organizations rely on social media to promote awareness of its programs. Many cyberattacks are conducted through the use of social media. Along with Internet usage, this policy would describe what content is deemed appropriate and prohibits the posting of any confidential information.

GLOSSARY SECTION

CYBERSECURITY - OTHER BASIC TERMS YOU SHOULD KNOW

ACCESS CONTROLS - *This is the IT Control that grants privileges to resources based on an employee's role in the organization on a need-to-know only basis. Failure to implement access controls can lead to an Elevation of Privilege attack.*

ATTACK SURFACE - *Any boundary that a hacker must navigate to get to or attack their desired target. This includes applications, smartphones, printers, computers, networks, employees, vendors, business partners, etc.*

DEVSECOPS - *This term mostly applies to software companies. It is the set of IT Controls applied to the development of secure software. Because software development companies take this* ***EXTREMELY SERIOUSLY****, the rest of us don't have to worry so much as long as we keep our software patched as advised by our software vendors.*

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS) - *An attack involving a network of devices working together to consume all of a host server's bandwidth rendering it unable to provide its intended function.*

ELEVATION OF PRIVILEGE (EOP) - *Exploitation of any vulnerability that allows a hacker or ordinary user to gain access to information they should not have access to.*

ENCRYPTION - *Encrypted data is protected by running it through a mathematical algorithm to lock or obfuscate the data so that only applications with the keys can read the data. HTTPS (secure) servers use encryption to avoid sending PII and credentials in plain-text which can be easily intercepted by cyber criminals with network eavesdropping tools. Modern browsers and servers can now enforce HTTPS encryption and it is quickly becoming the norm.*

EXPLOIT - *Actual cybercrime event.*

HACKER - *A cybercriminal.*

HACKTIVIST - *A cyberterrorist who thinks they are doing the world a favor by bringing down an unethical company. Profit is not their primary motivation.*

HACKER INDUSTRIAL COMPLEX - *Another name for the cybercrime supply chain infrastructure including the Dark Web. It is the collaboration of cybercriminals to monetize cybercrime.*

HONEYPOT - *A decoy server used to attract and trick a hacker. The more realistic the honeypot, the more can be learned about the hacker's modes, intentions, and even possibly their location and identity.*

INFORMATION DISCLOSURE - *This has nothing to do with Cybersecurity since no hacker is needed. It is when a user ignorantly or deliberately shares confidential, personal, or proprietary information outside of the organization. Information Disclosure is in direct violation of the Employee Code of Conduct.*

MALWARE - *This is a dangerous software program that a user inadvertently installs on their computer which provides a hacker with control over or access to the contents of their device. It is usually the result of a successful phishing attack.*

MAN-IN-THE-MIDDLE ATTACK - *This happens when a hacker gains control over a user's browser, application, or device and intercepts the user's credentials or other private information.*

PHISHING - *A social engineering attack using an email as the attack surface, usually to trick the user into downloading Malware.*

PII – ***Personally Identifiable Information.*** *This information contains certain identifiers (e.g., social security number), that can identify a person uniquely or if combined with other pieces of identifying information (e.g., date of birth), can allow someone else to successfully identify an individual.*

POLICIES - *This is an IT Controls word that refers to the definition of efficient and safe behaviors or interactions within an organization between all interfacing parts. Policies are simply the requirements which controls are meant to safeguard and guarantee.*

PPSI – ***Personal Private Sensitive Information*** *are records that are not easily accessible from public sources and can include someone's full name, social security number, driver's license, medical records, and/or financial information.*

REPUDIATION - *This provides the Hacker with a means of covering their tracks due to a failure of IT Controls to maintain an immutable audit trail.*

RISKS VS. ISSUES - *A risk is an undesirable event with a non-zero, but less than 100% probability. An issue is an undesirable event with a 100% probability, because it ALREADY happened. Risks can be anticipated and an attempt can be made to minimize them with an IT Controls process. Issues require impact mitigation and resolution via an Incident Response process.*

SOCIAL ENGINEERING - *A strategy used by hackers to exploit members of an organization with access privileges to the organization's resources to gain access to their desired target.*

SPOOFING - *A social engineering attack method where a hacker creates a look-alike application, site or device which a person believes to be the real thing and tricks the user into providing credentials or other private information.*

THREAT - *Potential ability to exploit a vulnerability.*

VULNERABILITY - *Gap or hole in a company's IT Controls - AKA Control Break.*

ZERO DAY EXPLOIT - *It is the first day a vulnerability exploit is detected. It starts the race between copycat cybercriminals and IT Security teams or vendors to close the vulnerability or break and minimize the damage to the stakeholders.*

ZERO TRUST - *This is the IT Control that defines and grants interaction privileges of devices and applications in a network to each other based on strict need-to-interact policies.*

WHAT OUR CLIENTS ARE SAYING...

As we have grown our technology company from a start-up idea into a thriving business, Cerini has been an indispensable partner for us, providing spot on accounting, impeccable advice and top-notch professionalism. I have peace of mind that my accounting needs are being addressed by the Cerini team.

Drew Stern, Founder & Co-CEO
Esquify, Inc.

Business Overview

Cerini & Associates, LLP is a full services accounting firm with a foundation built on value-added ideas and integrity. C&A is a leader in providing accounting and consulting services to the full spectrum of businesses, nonprofit organizations, and governmental entities. C&A services include, but are not limited to:

- *Accounting & Auditing*
- *Tax Compliance & Consulting*
- *Internal Audit Services*
- *Outsourced Accounting and CFO Services*
- *Mergers & Acquisitions*
- *Business Advisory*
- *Operational & Internal Control Reviews*
- *Tax Controversy Defense & Support*
- *Litigation Support & Special Projects*

C&A's staff takes pride in the quality of its work and operates with the technical ability of a much larger firm. C&A is also proud to have received an unqualified opinion during its last tri-annual peer review. The firm is affiliated with many professional organizations, including the: New York State Society of Certified Public Accountants, American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners.

GET IN TOUCH
(631) 582-1600
3340 Veterans Memorial Hwy.
Bohemia, NY 11716
www.cerinicpa.com

OUR PARTNERS

SCHOOL DISTRICTS

Diamond works primarily with the firm's school district clients focusing on internal controls, information technology assessments, and risk reduction strategies. She has over 25 years' experience and is committed to providing recommendations that help her clients meet their educational goals.

SHARI DIAMOND, CIA | SDIAMOND@CERINICPA.COM

ENTREPRENEURIAL

McWilliams has vast experience working with companies of all sizes and complex tax issues; this experience combined with his understanding of tax law allows for specialized advice in the areas of tax compliance, controversy, international taxation, and state and local taxes for these companies. Furthermore, he has extensive experience in business advisory services to help companies improve their organizational effectiveness and profitability

EDWARD MCWILLIAMS, CPA | EMCWILLIAMS@CERINICPA.COM

Roffi works closely with the firm's small business clients focusing on tax compliance, planning, accounting assistance and management advisory. She also is responsible for the firm's internal operations and finances.

KIMBERLY ROFFI, CPA | KROFFI@CERINICPA.COM

Sciacca has been providing consulting, tax, and accounting services for over 40 years to closely-held businesses with a concentration in the construction and real estate industries. He regularly consults regarding credit matters as well as representing them before various governmental and taxing authorities.

JOSEPH SCIACCA, CPA | JSCIACCA@CERINICPA.COM

NONPROFIT

Cerini focuses on nonprofit, education, and healthcare providers. With over 35 years of experience, he brings to each relationship a business acumen and focus that goes beyond what you traditionally find in an accountant. He is extremely responsive and is a strong advocate for his clients.

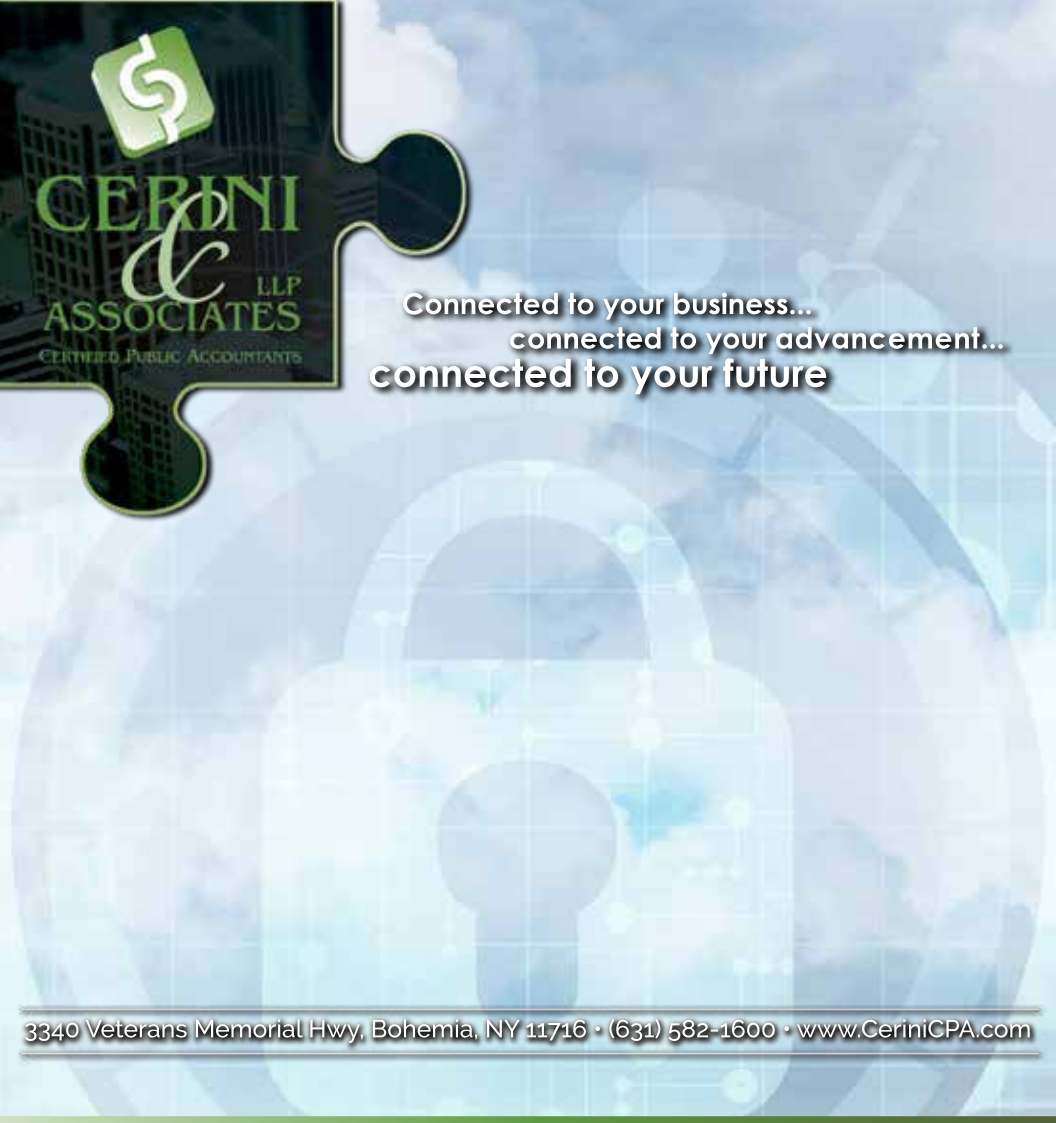
KEN CERINI, CPA, CFP, FABFA | KCERINI@CERINICPA.COM

Burke specializes in serving nonprofit and mid-sized business clientele. With over 20 years of experience, he works closely with many types of complex accounting, auditing, compliance, and general business matters that impact both the nonprofit and entrepreneurial communities.

MATTHEW BURKE, CPA, CFE | MBURKE@CERINICPA.COM

Quigley has been a member of Cerini & Associates' audit and consulting practice area since 2005 where she focuses on serving the firms nonprofit and employee benefit plan clientele. Tania has experience in performing financial statement audits and reviews, tax return preparation, cost report preparation and filing, retirement plan audits, and other consulting projects.

TANIA QUIGLEY, CPA | TQUIGLEY@CERINICPA.COM



THANK YOU TO OUR CONTRIBUTORS

CONNECTED TECHNOLOGY

Gallagher
Insurance | Risk Management | Consulting

MH&H Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

PUPFISH™ SUSTAINABILITY
Data Destruction, Electronics Recycling + IT Asset Liquidation Solutions

RoundTable TECHNOLOGY

STETSON cybergroup