CYBERSECURITY WHITEPAPER

BUILDING CYBERSECURITY IN SMALL AND MIDSIZE BUSINESSES

SPANNING

Victor O. Schinnerer & Company, Inc.

WITH ASSISTANCE FROM Microsoft

CONTENTS

EXECUTIVE SUMMARY

The rapid pace of technology innovation is clearly evident in all aspects of life. Advancements in mobility, social media, and cloud computing are changing the way people work, interact, and make purchases. For businesses, this trend brings increased growth and productivity—but it also brings added exposure to risk.

Always-connected businesses are conducting billions of online transmissions and transactions every day. With so much data online, businesses expose themselves to an increasing amount of cyber theft, online attacks, and electronic data breaches. Lost or stolen information can expose company secrets, disclose customer data, and reveal confidential employee information.

While the news media report on the data breaches of big corporations, small and midsized businesses are at risk as well. Cybercriminals assume that smaller business owners don't have the resources or necessary expertise that large companies have to defend themselves.

Although absolute security may not exist, *you can make a difference.*

According to the Online Trust Alliance (OTA), nearly 90 percent of cybersecurity breaches could have been avoided with the implementation of simple controls and security best practices.

This report outlines how the combination of modern and affordable technology, new cyber insurance coverages, and proper education enables business owners to better protect against business interruption and financial loss resulting from identity theft and malicious cyberattacks. These same measures can even help mitigate business risks associated with natural disasters and other non-malicious IT system failures.

KEYS TO SUCCESS

- Safeguard your business with modern technology
- Develop a response and recovery plan; consider cyber insurance
- Build a culture of security with your employees

CYBERSECURITY THREATS FACING SMALL AND MIDSIZED BUSINESSES

The rapid pace of technology innovation is evident in all aspects of life. Advancements in mobility, social media, and cloud computing are changing the way people work, interact, and make purchases. For businesses, this trend brings increased growth and productivity—but it also brings added exposure to risk.

Always-connected businesses are conducting billions of online transmissions and transactions every day. With so much data online, businesses expose themselves to an increasing amount of cyber theft, online attacks, and electronic data breaches. Lost or stolen information can expose company secrets, disclose customer data, and reveal confidential employee information. Further, malicious insider or outsider attacks can rapidly destroy crucial business data and impact business operations.

Cybercrime is rising at an epidemic level, resulting in a greater impact on small and midsized businesses (SMBs). While the news media report on the data breaches of big corporations, SMBs are at risk as well. Cybercriminals assume that smaller business owners don't have the resources or the necessary expertise that large companies have to defend themselves.

Newer forms of cyberattacks, like ransomware, are specifically targeting SMBs, using malware in bogus emails and freezing computer files until a ransom is paid.

Small businesses can be particularly vulnerable because they often have less sophisticated computer defenses. For example, 80 percent of small and midsized businesses don't use data protection, and less than half of them use email security, according to Intel Security.[1]

This whitepaper presents an approach to building a cybersecurity plan for your business. These recommendations are based on the Framework for Improving Critical Infrastructure Cybersecurity,[2] a collaborative effort between technology and insurance industries as well as the U.S. government. The cybersecurity framework represents a comprehensive compilation of effective cyber-defense processes, practices, and protocols available today. The goal of the framework is for organizations of any size to tailor and adopt it to fit their business circumstances and network configurations and to serve as a reference tool for managing cyber risks and threats.

> According to Intel Security, 80 percent of small and midsized businesses don't use data protection, and less than half of them use email security.[1]

[1] Simon, Ruth. "'Ransomware' a Growing Threat to Small Businesses." The Wall Street Journal. April 15, 2015.

[2] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. National Institute of Standards and Technology. February 12, 2014.

> *The Wall Street Journal* also reports that there are 34,529 known computer security incidents every day in the United States. At least 62 percent of these incidents involve breaches of SMBs — many of them Main Street firms which lack the technological sophistication enjoyed by larger retailers and other big companies.[3]

Managing Cyber Risk

Although absolute security may not exist, *you can make a difference.* This report outlines how the combination of modern-yet-affordable technology, cyber insurance coverage, and proper education enables business owners to better protect against business interruption and financial loss resulting from identity theft and malicious cyberattacks. These same measures can even help you mitigate business risks associated with natural disasters and other non-malicious IT system failures.

Safeguard your business with modern technology. With a modest investment in time and money, a significant portion of cyber risk can be avoided. Today's software applications and computing devices leverage built-in security, such as encryption and access controls, along with automated backup and restore to better protect business data.

Develop a response and recovery plan. Cyber insurance policies can provide response and recovery solutions when breaches do occur. Cyber insurance is not just about covering certain costs due to cybercrime. Many policies connect you to a data breach team to help with notification requirements, recovery and restoration efforts, network recovery and liability damages arising from a breach, and even lost income.

Build a culture of security. According to the Online Trust Alliance (OTA), nearly 90 percent of cybersecurity breaches could have been avoided with the implementation of simple controls and security best practices. Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. In addition, establish rules of behavior for how to handle and protect customer information and other vital data, and make security a daily priority.[3]

[3] Simon, Ruth. "'Ransomware' a Growing Threat to Small Businesses." The Wall Street Journal. April 15, 2015.

BEST PRACTICES TO REDUCE CYBER RISK TO YOUR BUSINESS

The first step in developing a cybersecurity strategy focuses on identifying, analyzing, and evaluating the risks to be managed. Risks in cyberspace are typically thought of as risks to digital (or electronic) data, which, if exploited or destroyed, could negatively impact an organization's economic well-being. The next step requires putting into motion protective and recovery solutions, as outlined in the following sections.

Second, upgrading to modern technology can greatly reduce the risk to your business. Most recommendations are easy for an organization to adopt. And, whether you're a small or large organization, you don't need to spend a fortune. Microsoft's Windows 10 and Office 365, for example, are affordable solutions for any business, and include many security enhancements built-in, like strong identity management and malicious software blocking, so there's no need to install additional security software to actively protect your data.

Finally, make sure you know what to do in the event of a cyberattack. While the preventative measures outlined in this whitepaper can help reduce a significant amount of cyber risk to your business, there may be certain risks simply outside of your control. To assist you in building a response and recovery plan, consider getting cyber insurance coverage and third-party backup. Speak to your insurance agent and discuss what policies might be right for you.

Steps to Minimize Cybersecurity Risk

UNDERSTAND WHAT IS AT RISK

01 MODERNIZE YOUR TECH

02 CONSIDER CYBER INSURANCE

03 EDUCATE EMPLOYEES

SAFEGUARD YOUR BUSINESS

To properly address cybersecurity, you need to have the functional capabilities to identify, protect, detect, respond, and recover:

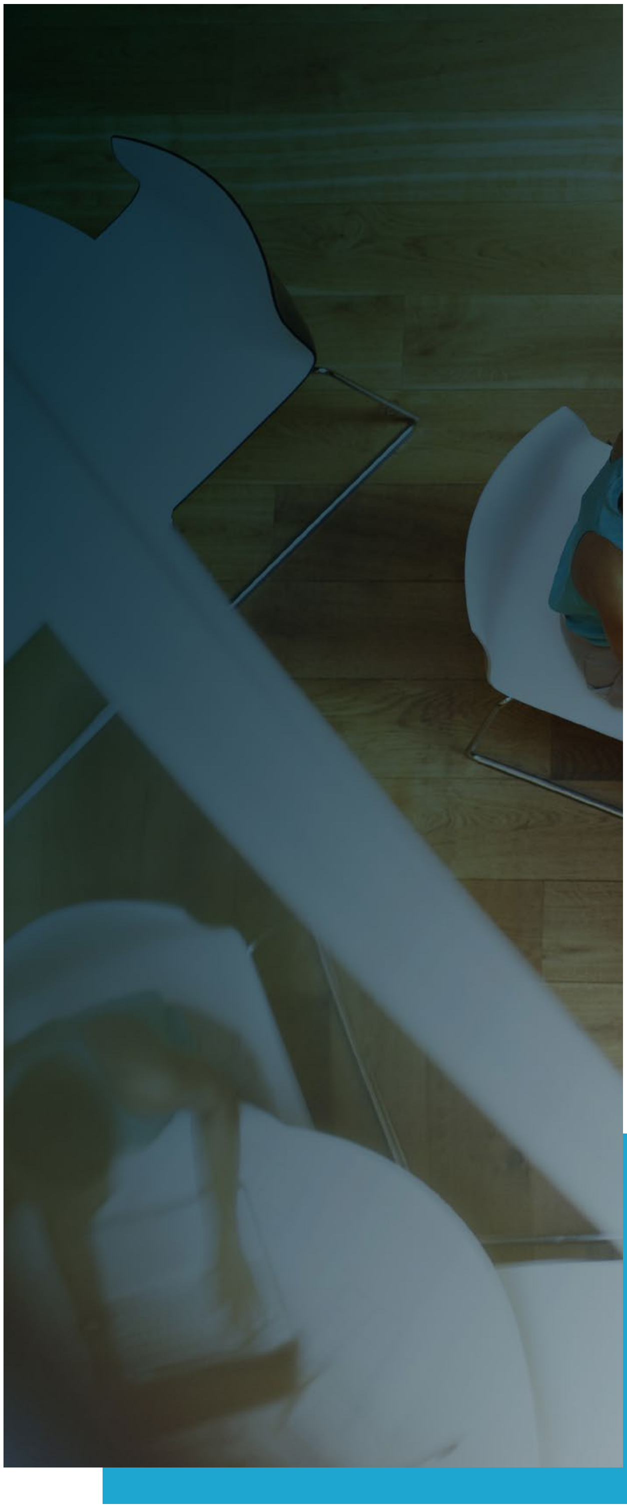
- Identify primary risk areas.
- Protect data and detect unauthorized access.
- Respond to breaches and recover quickly.

The National Institute of Standards and Technology framework is designed to help an organization define its current and desired cybersecurity state, to identify areas of need and current progress, and to offer advice on how to communicate to internal and external stakeholders about risks that threaten services.

For each functional capability, the framework tries to help organizations address:

- Where am I today?
- Where do I need to be?
- Gap analysis and action plan

As an SMB, it's critical to adopt the recommendations set forward in this framework to ensure that your assets and data are protected. But these recommendations can be done in workable components. What follows is a high-level list of recommendations, based on the cybersecurity framework.



IDENTIFY

It's important for an organization to understand which aspects of its business may be at risk. By understanding the business context, the resources that support critical functions, and the related cybersecurity risks, an organization is better able to focus and prioritize its efforts, consistent with its risk management strategy and its business needs.

Recommendations

To identify how your business may be at risk, create inventory checklists and develop an overview of cyber risk management, with an analysis of technology and tools that may be outdated and can put your business at risk.

Know your data. A critical first step in enhancing your data security is to identify what data you have, along with how your data is managed and secured. You should be able to identify what data is collected and which people, apps, and devices have access to that data. You should have a second copy of your data available for recovery. You should have a thorough inventory of the kind of information you have, how much of it you have, and where you have it. This includes customer and employee personally identifiable information (PII), such as financial, account, and salary information, in addition to other business data, like trade secrets, marketing plans, and new product specifications.

Know your portable devices. Theft and accidental loss of laptops, smartphones, and tablets are leading causes of compromised data. It is crucial that these devices are inventoried and centrally managed. Thus, in the event of a breach, the devices can be remotely secured and the protected information can be rendered unreadable and unusable.

Know your team. Everyone is accountable for managing cyber risks, including temporary workers and contractors. Have you implemented a sound internal communication and training strategy on the protection and proper use of sensitive data, including how to recognize and report security threats? Have you integrated cybersecurity into your employee orientation, with an emphasis on the consequences of sharing passwords, falling for email phishing scams, exposing laptops and USB storage devices to theft, and otherwise neglecting to observe data security policies?

Know your vendors. When entrusting personal information to third parties, implement reasonable measures to ensure that they have the capacity to protect this information. This means selecting only service providers which are capable of maintaining safeguards (equal to or better than yours) for personal information, and it means contractually requiring them to maintain such safeguards. You should also mandate that your vendors show proof of insurance to provide you with protection if they are the cause of loss.

Know your budget. Insurance is an important weapon in this war. According to the Ponemon Institute, the average security breach costs organizations almost $200 for each stolen record, or about $5.5 million for the typical company breach. A claim of that size could cripple a business which doesn't carry adequate insurance coverage. Ideally, it never gets to that point.

As part of identifying which assets and data could be attacked, an organization should also assess the potential impact of the data falling into the wrong hands. For example, do employees know how to protect this data? How/when can a breach be discovered? What is the first move in the event of a breach?

The following sections can help to answer these questions.

PROTECT AND DETECT

Protecting business data—and detecting cyberattacks or other unauthorized access to your data—is of paramount importance. Unfortunately, too many businesses still rely on older, outdated technologies, which expose SMBs' data to unnecessary risk and expose them to potential threats. The good news is that Office and Windows-based devices have built-in, enterprise-class security capabilities.

Protect

To properly protect your online data and digital information, consider the following:

Data storage and backup. Storing and backing up digital information properly is a must. Businesses can lose countless hours and dollars trying to restore compromised or lost data—often to no success.

Data storage considerations must include security, privacy, and compliance requirements. Depending on your industry, you may need various levels of admin and user controls, including e-discovery, legal hold, data loss prevention, and backup and recovery, to help you meet these requirements.

Managing them on your own requires expertise. However, today's cloud-based storage and backup solutions have enterprise-class security and privacy controls built-in, making them more cost-effective (and a wise investment) for small businesses.

User-access controls. Businesses today need to be able to connect employees to the data they need—wherever they are. The challenge however, is to enable your people to be productive anywhere, while maintaining the peace of mind that your critical business data is protected and secure. It's important to restrict access to data based on business needs only and to restrict levels of access to the right employees—on the right devices.

Controlling access to devices, applications, and data requires the ability to confidently authenticate the user and to manage business rules and permissions that dictate access rights. Weaknesses in authentication can lead to security infractions or to inappropriate granting of access.

Modern technologies, such as the Microsoft Enterprise Mobility + Security (EMS), allow you to use rule-based policies to protect data by denying or allowing access, based on combinations of user, device, and data properties. For example, rules can be set so that one folder may be accessed by an employee from a computer

TOP 5 RISKS OF USING OUTDATED TECHNOLOGY

- **Crashes and system downtime.** Time spent fixing IT issues rather than on the business.
- **Increased costs.** Money spent repairing technology problems instead of on company growth.
- **Decreased productivity.** Employees focused on resolving IT concerns and not on business tasks.
- **Security holes.** Cyberattack vulnerabilities rather than defenses.
- **Legal and regulatory compliance risks.** Potential fines from auditors, as a result of unsupported software.

but not from a mobile device, or a rule can be set so that the same folder can only be accessed by users with authentication. Users should be able to define who can open, modify, print, forward, or take other actions with their information—from emails to documents—and to prevent inadvertent sharing with unauthorized people. This control needs to apply to all types of information across all major platforms, particularly the cloud.

Use encryption technology. Every business should take steps to safeguard its information from unauthorized use, whether caused by accidental loss of mobile devices and laptops or by illegitimate access to sensitive data.

Devices used for business of any size should come with TPM (Trusted Platform Module). TPM is an international industry standard for microchips that are built into newer computers to store cryptographic information, such as encryption keys that protect your data. With TPM, encryption can make data indecipherable to unauthorized users. It provides enhanced protection against data theft, especially in an increasingly bring your own device (BYOD) workplace culture, where such devices can be outside of a secure environment.

To fully utilize encryption, consider upgrading to modern devices and operating systems. With Windows 10, for example, you can use built-in BitLocker Drive Encryption, to help block hackers from accessing data stored on the device.

Device and mobile workforce management. Modern businesses are taking advantage of the latest computer hardware and devices. BYOD provides a new way for business owners to accommodate different work styles and to save costs.

Allowing employees to work from multiple locations and, in some cases, with their own devices can be a great motivator and can help smaller businesses attract and retain the talent they need. The challenge, however, is to ensure that BYOD doesn't compromise the quality of your business capabilities or security.

The ability to access data and apps on mobile devices is essential for modern businesses, but those apps and devices need to be managed and kept up to date. Additionally, it's likely that business users have two or more devices. Does your business make it easy for users to sync data from their work folders to authorized devices?

Consider cloud-based applications that help empower a mobile workforce. When doing so, make sure that mobile device management (MDM) solutions would also help protect against data breaches, should one of your team members lose a mobile device. You should be able to:

- Lock the device to restrict access.
- Reset a user's PIN to enable access, after the device is found.
- Wipe data from a device that can't be located.

Create strong passwords. Passwords are the first line of defense against break-ins to your online accounts and computer, tablet, or phone.

Poorly chosen passwords can render your information vulnerable to criminals, so it's important to create strong passwords. Criminals often use automated programs to break into accounts guarded by simple passwords, such as "password" or "12345678." Strong passwords are long phrases or sentences that mix capital and lowercase letters, numbers, and symbols. They are easy for you to remember but difficult for others to guess.

Look for new devices with fingerprint authentication. Many devices now come with native fingerprint-based biometric options for authenticating user identities. Instead of typing passwords, users touch to sign in.

Detect

There are many ways that criminals exploit the Internet—fraudulent scams, malicious attacks, and unauthorized access to sensitive data—that could put you, your employees, and your customers at further risk.

Online criminals can use sophisticated technology to try to gain access to your computer. They can also use something simpler and more insidious, such as social engineering, which exploits your trust to gain access to your computer and sensitive personal information.

To help safeguard your business against online fraud, take the time to be safe when connected to the Internet. Make sure you and your employees understand how to recognize phishing scams and how to guard against malware.

Phishing scams use email, text, or social network messages which seem to come from a reputable organization, like your bank or a favorite charity. These messages are often so realistic that it can be difficult to tell that they are not legitimate.

In a phishing scam, a convincing message entices you to divulge sensitive information, like an account number or a password. Or it might ask you to call a phony toll-free number or to click a link that goes to a fake webpage, where you're asked to reveal personal data.

There are other forms of fraudulent scams that you and your employees should watch out for, including rogue security software, fake technical support, fraudulent contents and winnings, and financial scams. Criminals try to install malware on computers that haven't been updated, by exploiting older weaknesses in the software. When it comes to malware, the best defense is to keep all software up to date, including your web browser, operating system, and word processing and other programs. In the event of a ransomware attack, the best defense is to be prepared to quickly restore from the "last known good" state.

Recommendations

- **Install antivirus and antispyware software from a trusted source.** Windows 10 includes built-in antivirus and antispyware software, so there's no need to install additional security software to protect your machines.
- **Protect your wireless router with a strong password.** Never turn off the firewall on your computer. Don't follow the instructions of unsolicited callers or let them take control of your computer.
- **Think before you click links or call a number in a message.** Even if you know the sender, the links, phone number, and sender's identity could all be deceptive. Instead, confirm that the message is genuine, using a different device and another account.

Best Practices for Protect & Detect

Deploy affordable, modern technologies built specifically for small and midsized businesses, allowing you to:

- Properly back up and enable fast restore of digital data
- Control employee access to data
- Manage devices and your mobile workforce
- Create strong passwords

Educate yourself and your employees about:

- Phishing detection
- Guarding against malware

RESPOND AND RECOVER

As part of an overall cybersecurity plan, SMBs need to develop and implement a plan that identifies the appropriate response to a detected cybersecurity event, including how to communicate to employees, vendors, and customers who may be affected. In addition, it's important to maintain plans for resilience and to quickly restore any data, capabilities or services which were impaired or destroyed by a cybersecurity event.

Recommendations

Meet with your insurance agent. Often, the unknown creates the greatest concerns for SMBs. Insurance carriers have the experience and expertise to provide an overview of risks to business owners and the costs associated with those risks, including costs of notifying those affected, costs to re-create the data, and costs of system restoration.

Schinnerer Cyber Protection Package – From the simple application to the comprehensive coverage, the Schinnerer Cyber Protection Package (CPP) was designed for SMBs. The CPP is simple to execute and provides broad coverage to protect against digital crime, breach liability and breach rectification.

From criminals tricking you into paying false invoices, to liability arising from lost information, to income loss during business interruption, the Schinnerer Cyber Protection Package has you covered. And most importantly, you don't have to go it alone. With the Schinnerer CPP, SMBs have access to a cyber breach team that provides expert advice on legal reviews, forensic IT services, and the future risk of legal action or lawsuits. The breach team provides resources to guide an SMB through various regulations, notifications, system recovery processes, and public relations – all invaluable at the time of a cyberattack.

Be prepared to quickly recover data. When you migrate to Office 365, your responsibility to protect your company's data remains the same. Microsoft provides strong platform protection to ensure that they never lose your data; however, they can't protect your data from malicious or unintentional behavior that appear to be legitimate requests. Users with proper access rights, malicious intruders and malware, like ransomware, all can change or destroy data.

Third-party backup and recovery providers can help mitigate the business continuity risks associated with data loss and cybersecurity attacks. SMBs should consider SaaS backup services that are easy to acquire and manage and focus on solutions that provide granular, rapid restore to reduce cost and recovery time associated with any data disaster.

Best Practices for Respond & Recover

Speak with your insurance agent or broker, and see how cyber insurance might be a good solution for your business, covering certain costs related to:

- Services to notify those affected
- Legal reviews and forensic IT service
- ID theft recovery and monitoring services
- Legal action/lawsuits
- Data re-creation
- System restoration
- Indirect costs, such as operational expenses and business income loss

CYBERSECURITY SOLUTION OVERVIEW

SOLUTION	OVERVIEW	CAPABILITIES
Office 365	Cloud security with Office 365 integrates built-in security, privacy controls, compliance with industry standards, and transparent operations. Office 365 is a security-hardened service and is a culmination of best practices from two decades of building enterprise software and managing online services for an integrated software-as-a-service solution. At the service level, Office 365 uses the defense-in-depth approach to provide physical, logical, and data layers of security features and operational best practices. In addition, Office 365 offers enterprise-grade user and admin controls to further secure your environment, through a low-cost solution.	■ Cloud Storage ■ Security, privacy, and compliance ■ Enterprise-class email
Windows 10	Windows 10 is the most secure Windows ever and has more built-in security protections to help safeguard you against viruses, phishing, and malware. Windows 10 actively addresses modern security threats with advancements to strengthen identity protection and access control, information protection, and threat resistance. Automatic updates enable you to ensure that your systems stay current.	■ Multilayered encryption ■ Advanced malware and spam protection ■ Biometric and multifactored authentication
Microsoft Enterprise Mobility + Security	Microsoft Enterprise Mobility + Security is the only cloud solution built to deliver access to apps and data across all devices, while helping to keep your business secure. This suite enables SMBs to cost-effectively license Microsoft Enterprise Mobility cloud services for all its users, enabling Microsoft Azure Active Directory Premium to deliver robust identity and access management from the cloud, in sync with your existing on-premises deployments. As part of the suite, Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud.	■ Identity management ■ Mobile management ■ Information protection

CYBERSECURITY SOLUTION OVERVIEW

SOLUTION	OVERVIEW	CAPABILITIES
SPANNING BACKUP FOR OFFICE 365	Spanning Backup for Office 365 is the most scalable and secure, purpose-built backup and recovery solution for Microsoft Office 365. Spanning Backup for Office 365 delivers automated, point-in-time back up for Mail, Calendar, OneDrive for Business, and SharePoint Online, and enables administrators and end users to quickly find and restore lost data. Spanning's SaaS service is SSAE 16 SOC 2 and HIPAA compliant, leveraging strong encryption and federated authentication.	■ Third-party backup ■ Daily, automated backups ■ Rapid, granular restores
Victor O. Schinnerer & Company, Inc.	Schinnerer Cyber Protection Package provides financial protection against cyberattacks with skillfully underwritten coverage. The coverage is designed to scale, so protection continues seamlessly as your business grows.	■ Step-by-step guidance to respond to a cyberbreach, including reporting and notification requirements ■ Third-party liability protection ■ Access to cloud-to-cloud automated backup and restore solutions, and to a network of restoration-service providers ■ Reimbursement of associated costs ■ Business-interruption minimization

CYBERSECURITY READINESS CHECKLIST

Cybersecurity threats are real, and businesses must implement the best tools and tactics to protect themselves, their customers, and their data. Following is a checklist summarizing the key recommendations in this whitepaper.[4]

01 IDENTIFY WHAT DATA IS AT RISK. □

Create an inventory checklist and develop an overview of all data you collect, and understand what people, apps and devices have access to that data. Consider (1) customer data (PII, transaction data, account numbers, spend history, etc.), (2) employee data (PII, credit files, payroll, HR, salary, etc.), (3) financial data (company account information, online access credentials, etc.), and (4) other data, such as trade secrets, marketing plans, and new product specifications.

02 PROTECT YOUR DATA. STORE AND BACKUP TO THE CLOUD. □

Regularly back up the data on all computers and in Office 365. Critical data includes word processing documents, electronic spreadsheets, customer databases, financial files, human resources files, and accounts receivable/payable files. Back up data automatically at least daily, and store in a secure cloud that can enable fast, accurate restores.

03 CREATE A PROCESS TO KEEP APPS UP TO DATE. □

Adopt modern technology that enables you to automatically update your software so your anti-virus software is always current. Keep clean machines: having the latest versions of applications, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

04 SECURE YOUR NETWORKS (WI-FI, FIREWALLS). □

Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

[4] Federal Communications Commission. "Cybersecurity Tip Sheet."

05 ENSURE YOU ENCRYPT YOUR DATA. □

Whether in storage, in transit across networks and within all business devices, make sure your data is encrypted and safely transmitted.

06 IMPLEMENT A MOBILE-DEVICES MANAGEMENT PLAN. □

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

07 RESTRICT USER ACCESS TO ONLY THE DATA THEY NEED. □

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

08 CREATE A RESPONSE AND RECOVERY PLAN. □

Speak to your insurance agent about purchasing the Schinnerer Cyber Protection Package that provides broad coverage to protect against digital crime, breach liability and breach rectification. Acquire backup and recovery services for your SaaS data that require little effort, but deliver reliable, point-in-time restore of critical data after any cybersecurity attack occurs.

09 EDUCATE YOUR EMPLOYEES ON CYBERSECURITY AND BEST PRACTICES. □

Create a training plan, keep records for each employee's participation and have them acknowledge their commitment to security. Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

10 GUARD AGAINST PAYMENT FRAUD. □

Employ best practices on credit cards, and make sure your card-readers are using modern EMV chip-technologies.

ABOUT SCHINNERER

With more than 46,000 insureds, Victor O. Schinnerer & Company is one of the largest and most experienced underwriting managers of specialty insurance programs in the world.

Schinnerer Cyber Protection Package

ABOUT MICROSOFT

Microsoft is the leading platform and productivity company for the mobile-first, cloud-first world. Its mission is to empower every person and organization the planet to achieve more.

Microsoft Office 365

Microsoft Enterprise Mobility + Security

SPANNING

Spanning Cloud Apps is the leading provider of backup and recovery for SaaS applications, protecting thousands of organizations from data loss due to user error, malicious activity and more. We are the only global provider of powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning is the most trusted cloud-to-cloud backup provider with millions of users around the world.

Spanning Backup for Office 365

501 CONGRESS AVE, SUITE 200
AUSTIN, TEXAS 78701
P +1.512.236.1277

SPANNING.COM