SONATA BANK FINANCIAL WELLNESS SERIES

What Small Business Owners Need to Know About Cyber Safety

sonata bank

IMPORTANT DISCLOSURE

For Informational Purposes Only

The information provided in this eBook, “WHAT SMALL BUSINESS OWNERS NEED TO KNOW ABOUT CYBER SAFETY,” is for general informational and educational purposes only. While we strive to keep the information up-to-date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this eBook for any purpose.

This eBook is not intended as a substitute for professional advice. The field of cybersecurity is complex and constantly evolving, and individual situations can vary greatly. Therefore, we strongly recommend that readers consult with qualified cybersecurity experts or legal advisors for personalized guidance tailored to their specific circumstances.

Any reliance you place on the information in this eBook is strictly at your own risk. We will not be liable for any loss or damage arising from the use of any information contained within this publication.

Please note that cybersecurity laws, regulations, and best practices may change over time. It is the reader’s responsibility to stay informed about current developments in cybersecurity and to comply with all applicable laws and regulations.

By reading and using this eBook, you acknowledge that you have read and understood this disclosure statement.

IMPORTANT DISCLOSURE

Important Notice Regarding Insurance-Related Content

The information provided in this eBook regarding cybersecurity liability insurance and other insurance-related matters is intended for general informational purposes only. It should not be construed as professional insurance advice or a recommendation for any specific insurance product or service.

Every business has unique needs and risk profiles, and insurance coverage should be tailored accordingly. We strongly recommend that readers consult with a licensed insurance professional or broker to discuss their specific circumstances and obtain personalized advice on appropriate insurance coverage.

The authors, publishers, and distributors of this eBook are not insurance professionals and do not provide insurance services. We make no representations or warranties about the suitability, reliability, or accuracy of the insurance-related information contained herein.

Insurance policies, terms, conditions, and exclusions can vary significantly between providers and are subject to change. It is crucial to carefully review any insurance policy before purchase and to understand its terms and limitations fully.

The decision to purchase any insurance product should be based on your individual needs, financial situation, and consultation with qualified professionals. This eBook does not create any form of insurance relationship or coverage.

By reading and using the information in this eBook, you acknowledge and agree that the authors, publishers, and distributors shall not be held responsible for any errors, omissions, or any actions taken based on the information provided.

INTRODUCTION

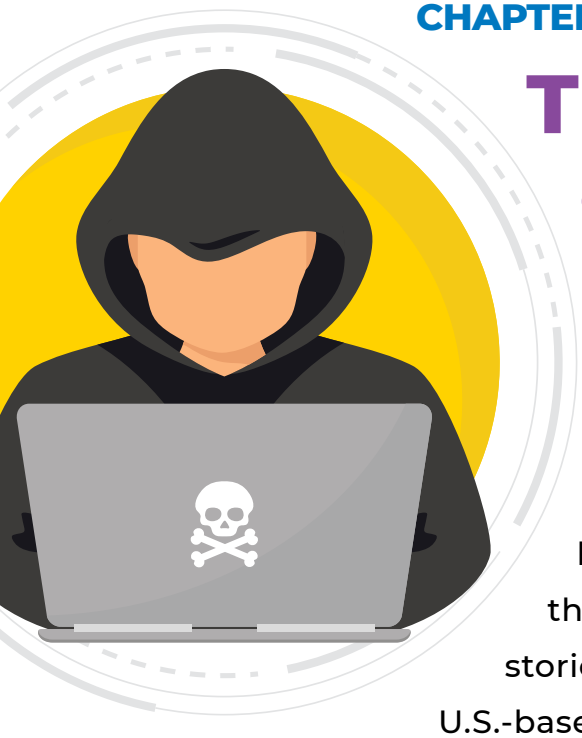
Think Your Small Business is too Small for a Cyberattack?

You might be surprised to learn that 37% of all companies hit by ransomware attacks had fewer than 100 employees and 82%* of ransomware attacks are targeted at small businesses. Aside from the liabilities from the cyberattack, a whopping 60%* of small businesses have to close within six months of an initial cyberattack.

Did you know that 51% of small businesses have **zero cybersecurity measures*** in place at all? Customers only need to get burned once before they take their business elsewhere. Fifty-five percent* of U.S. consumers polled said they were less likely to continue doing business with companies that are breached.

In recognition of October being National Cybersecurity Awareness Month, Sonata Bank is taking this opportunity to provide you with the information you need to protect the small business you are working so hard to grow and flourish.

CHAPTER ONE



The True Story of 1 Small U.S. Business, 1 Year, 3 Cyberattacks

Especially since Covid, cyberattacks on small businesses have escalated. Experts estimate that increase is 600%.* These are three true stories of cyberattacks that happened to one small U.S.-based industrial business within one year's time.

THE CHECK-WASHING ATTACK:

Recently, DeDe, a small fabrication shop's accountant, watched as $60,000 in attempted "check washing" was being run through her company's national bank account. DeDe's business owner, Brian, was out of the country, but DeDe caught the fraud in real time. She was able to correct it because she already had "positive pay" set up with their bank. Positive pay is the automated cash-management service where the bank matches all checks issued by her company with the checks that get presented for payment, and then sends her alerts to validate the approved checks.

How does "check washing" occur? Criminals have many ways to access a company's checking account information. This can occur when criminals steal paper-based bank statements from your

mailbox. In this case, the accountant said they hadn't used paper-based bank statements in many years to protect against fraud. DeDe believes it was a disgruntled ex-employee who shared his final paycheck's information with someone who then recreated checks using a graphic design software that included her company's business name, business bank account number, and routing number.

THE PHISHING ATTACK:

In another situation, DeDe became the victim of a "phishing attack." She clicked on an emailed link or attachment at some point that she shouldn't have. Bad actors then accessed her Microsoft Outlook, rewrote the "rules" for how her emails were routed, and all of her accounts receivable emails were then rerouted to the criminals' own account. This resulted in their business losing a $30,000 payment at year's end, which got paid to the criminals. The client, who inadvertently paid the criminals, refused to make good on the money they owed, so the fabrication company had to take it as a loss. This was when they made the unfortunate discovery that their business

insurance had a loophole to avoid covering the fraud. Since that time, they have secured a new business insurance policy that covers them for situations like this one.

THE SOCIAL ENGINEERING ATTACK:

The third incident their fabrication shop endured was a "social engineering" attack. Social engineering occurs when scammers use the personal information they glean from your social media websites to sound convincing. Again, Brian the owner was out of town. Before he left for his trip to Ireland, he created an email auto-reply message that stated, "***I'm out of the country, please contact DeDe at (805) 555-5555 until my return on October 31, 2024.***" DeDe received an email stating that Brian and his wife Tammy had their money stolen and they would need DeDe to click the emailed link to send him $10,000. The criminal used DeDe's boss's wife's real name, which made the request sound more credible.

"My first thought was that it sounded semi-legit since they knew Tammy's first name, so I called his parents and asked if they had heard from him," DeDe shared. "They said they had just spoken with Brian and he was having a great time. That's when I knew for sure my spidey-senses were right— I was being spoofed. I alerted Brian, who immediately had me go into his email auto-reply and remove the information that he was out of the country."

While you may think it is unusual for one business to encounter this many cyberattacks in 12 months' time, cyber criminals view small businesses as low-hanging fruit for faster— albeit less profitable— financial hits.

CHAPTER 2:

What Can You Do to Protect Yourself from Cyber Fraud?

According to the Hiscox Cyber Readiness Report, the average investment in cybersecurity protection for a small business can range from $6,000 to $24,000 per year, with 5% to 20% of the overall IT budget funding cybersecurity. Deloitte reported that 22% of small businesses grew their cybersecurity spending post-COVID-19 thanks to the massive increase in threats.

It's unrealistic to expect that you will have full protection against all cyberattacks. However, you can reduce your exposure and the risks associated with these worrisome attacks. Here are some recommendations for a small business:

Secure Passwords: All employees must create strong passwords. There are automated password generators, but if you opt to create your own, the National Institute of Standards and Technology (the NIST) defines a "strong password" protocol as including the following characteristics:

- User-generated passwords should be at least eight (8) characters; machine-generated passwords should be at least six (6) characters)
- Does not use personal information
- A unique password for every account
- Special characters are acceptable, but no longer required. Breached password analyses indicate that special characters weren't as beneficial as initially thought.

Adopt a "Zero-Trust Security Policy": When you deploy a zero-trust model, no one – inside or outside of the network – is trusted by default. This approach requires:

- Continuous verification of user and device identity
- Strict access controls
- Role-based access to data
- Micro-segmentation of the network, which limits the impact of a potential breach

Automate Your Incident Response: By investing in automation tools, you can benefit from the following:

- Predefined responses to detected threats
- Reduced response time
- Minimized impact from cyber incidents

Secure Internet of Things (IoT) Devices: IoT devices such as sensors, actuators, or appliances that connect wirelessly to your network can transmit data, so they are easy entry points for cyberattacks. Ensure that they are:

- Securely configured
- Regularly updated
- Monitored for potential vulnerabilities

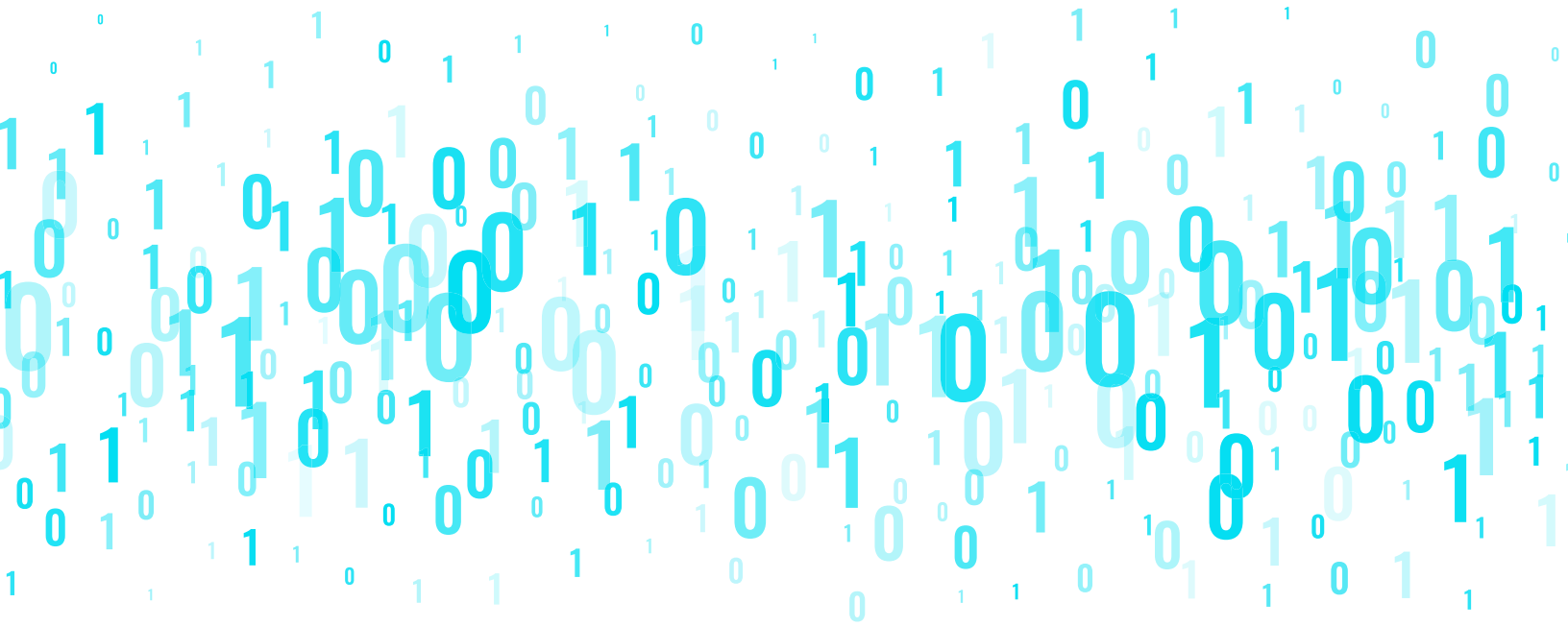
Foster an Employee Cybersecurity-First Culture with Awareness Training: Encourage your employees to be proactive about security, report suspicious activities, and engage with security policies and updates. Subscribe to a cybersecurity training that requires your employees pass the tests and simulation situations they are given to familiarize them with emerging threats, including:

- Social engineering tactics
- Deep fakes
- Advanced phishing techniques

Employ Data Compliance Tools and Processes: Regulations are constantly evolving, so you need to be managing customer data in adherence with the following regulations:

- **General Data Protection Regulation (GDPR):** This is a significant piece of legislation in the EU that protects citizens' data privacy rights. It also sets out stringent rules for exporting personal data outside the EU.

- **California Consumer Privacy Act (CCPA):** This law grants California residents the right to know what personal data is being collected and shared by businesses and provides them rights over their personal information.
- **Health Insurance Portability and Accountability Act (HIPAA):** It is a US federal law that requires the protection and confidential handling of sensitive health data.
- **Payment Card Industry Data Security Standard (PCI DSS):** This PCI compliance standard applies to any business that handles credit card transactions and requires strict security measures to protect against data theft.
- **Sarbanes-Oxley Act (SOX):** A US law that mandates strict auditing and financial regulations for public companies to protect shareholders.
- **The Federal Information Security Management Act (FISMA):** This US legislation requires federal agencies to implement security programs to protect data and information systems.
- **Children's Online Privacy Protection Act (COPPA):** This U.S. law restricts the collection of personal data from children under 13.
- **The Personal Information Protection and Electronic Documents Act (PIPEDA):** A Canadian federal law that sets privacy standards for how private businesses handle personal data.
- **Asia-Pacific Economic Cooperation (APEC) Privacy Framework:** This is a set of principles and commentaries on privacy protection standards for APEC member economies.
- **Australian Privacy Act 1988:** This Australian regulation governs how personal data is handled.



Deploy AI and Machine Learning Tools: The key advantage to these tools is that they identify and react to cybersecurity threats in real time. The advantages include:

- Identifying unusual patterns or behaviors
- Enabling faster response times to minimize attack damage

Utilize An XDR Advanced Security Solution: This solution integrates multiple security products into one cohesive system. These advantages include:

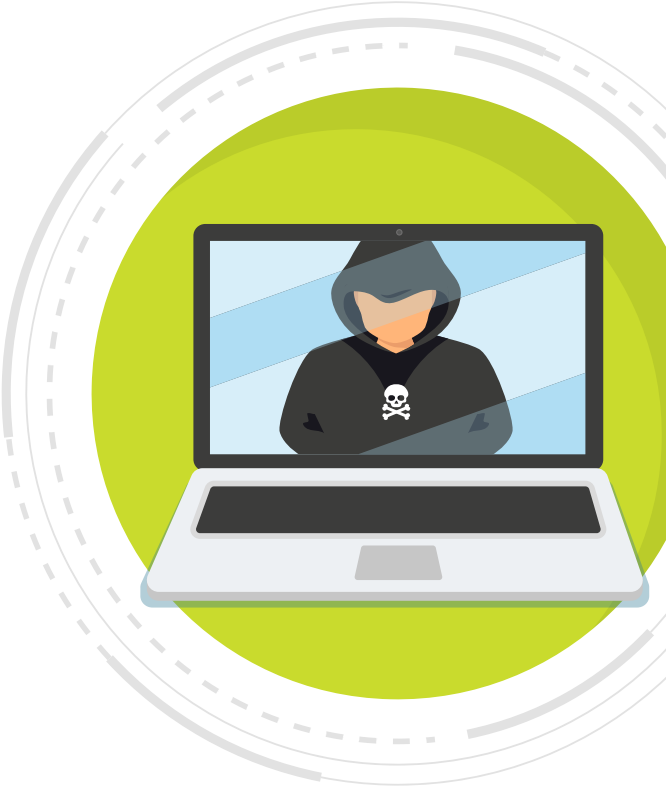
- Broader visibility
- Faster detection
- More automated responses across your business's entire IT infrastructure

Adopt a Third-Party Risk Management Framework (or a TPRM): Using third-party vendors creates additional cybersecurity risks. The purpose of a TPRM framework is to reduce the likelihood of data breaches, costly operational failures, vendor bankruptcy, and to meet regulatory requirements. A TPRM should include the following components:

- A vendor risk assessment program
- Compliance gap detection (especially for critical regulations like PCI-DSS)
- Third-party vulnerability detection
- Security questionnaire automation
- A remediation program
- Report generation feature for keeping stakeholders informed of TPRM efforts

Cyber frameworks mapping to TPRM requirements and security controls can include:

- NIST CSF
- ISO 27001
- ISO 27002
- ISO 27019
- ISO 27036
- NIST RMF 800-37



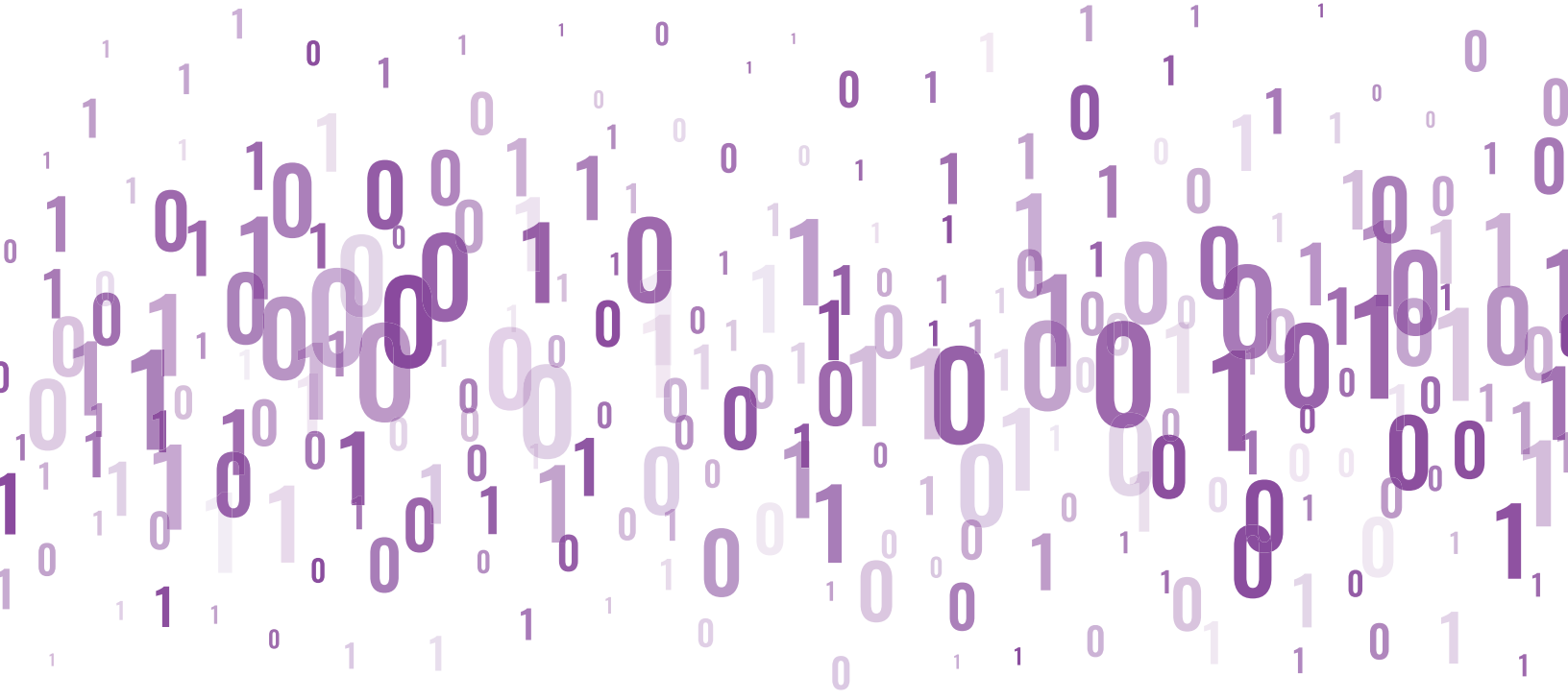
Monitor Insider Threats: By installing employee behavior analytics software, any anomalies in employee behavior will be detected. These include:

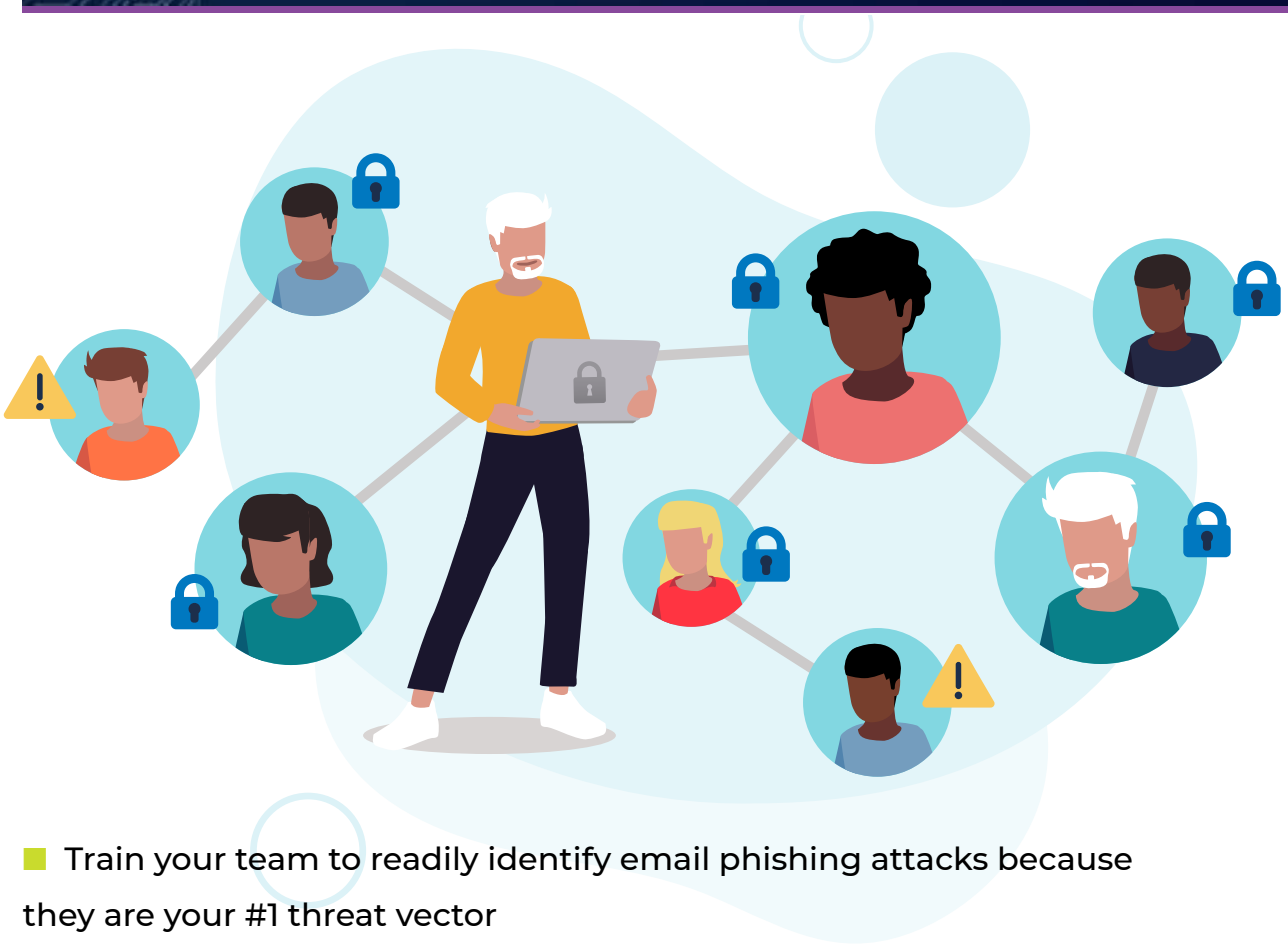
- Unusual access patterns
- Data transfers, or
- Other suspicious activities

A Truncated List of Best Practices for a Small Business

- Invest in a “Managed Service Provider” (MSP) to perform penetration testing and ensure your vulnerabilities are all thoroughly covered. (A penetration test, or “pen test,” is a security test that launches a mock cyberattack to find vulnerabilities in a computer system; penetration testers are skilled in the art of ethical hacking, which is the use of hacking tools and techniques to fix security weaknesses rather than cause harm)
- Secure your Wi-Fi network with WPA3 encryption (the most secure wireless encryption protocol)
- Update your router firmware
- Install a VPN for your employees
- Assign MAC (Media Access Control) filtering so each device has an approved MAC address to connect to your Wi-Fi
- Create a separate isolated guest network if you have customers or visitors who come to your business location and need internet access
- Institute strong password protocols in addition to 2FA (2-Factor Authentication) to validate the identities of your users
- Encrypt your sensitive data

- Employ role-based access controls (RBAC) so that the access to your sensitive data and systems is only for the employees who need it to perform their work duties.
- Secure an incident response plan to respond to any cybersecurity intrusions
- Perform simulations to ensure your team is prepared
- Secure a backup and recovery solution and plan so that you don't lose any of your data
- Back up your data regularly to a secure location
- Ensure your remote users are using a "Virtual Private Network" software (VPN)
- Update your apps and devices' software as you are alerted; many successful attacks work because apps and devices are not patched when they need to be





- Train your team to readily identify email phishing attacks because they are your #1 threat vector
- Protect your small business from financial devastation with cyber liability insurance

If there is a particular time of year when your business is swamped with work or overtime hours, the scammers will exploit that vulnerability and know that is the time to strike. For example, for accountants, scammers know it's the 30 days leading up to April 15th that they will be the most vulnerable. For some companies, it's holiday weekends and summer vacation periods when there's a skeleton crew. If a company's fiscal year is July to July, scammers know that company will be slammed with year-end inventory validation and accounting at fiscal year's end. When you're the most overworked or understaffed, that's when you must be the most hypervigilant.

These strategies will better prepare small businesses for the evolving landscape of cyber threats in 2025.

What You Need to Include in Your Cybersecurity Liability Insurance

Your cybersecurity insurance policy should include the following key components so that you are covered by various cyber risks:

- **Data Breach Coverage:** This covers the costs associated with responding to a data breach, including forensic investigations, customer notifications, legal assistance, and credit monitoring for affected individuals.

- **Business Interruption:** If a cyberattack disrupts business operations, this coverage compensates for lost income during the downtime, as well as any extra expenses incurred to keep the business running.

- **Cyber Extortion and Ransomware:** This coverage helps if the business falls victim to a ransomware attack or other cyber extortion schemes, covering ransom payments (if permissible) and the cost of negotiating with hackers.

- **Legal and Regulatory Fees:** Covers the costs of legal defense in the event of lawsuits or regulatory penalties related to the cyber incident, including violations of privacy laws such as GDPR or CCPA.

- **Third-Party Liability:** Protects against claims made by third parties, such as customers or partners, for damages resulting from a cyberattack on the business that impacts their data or systems.

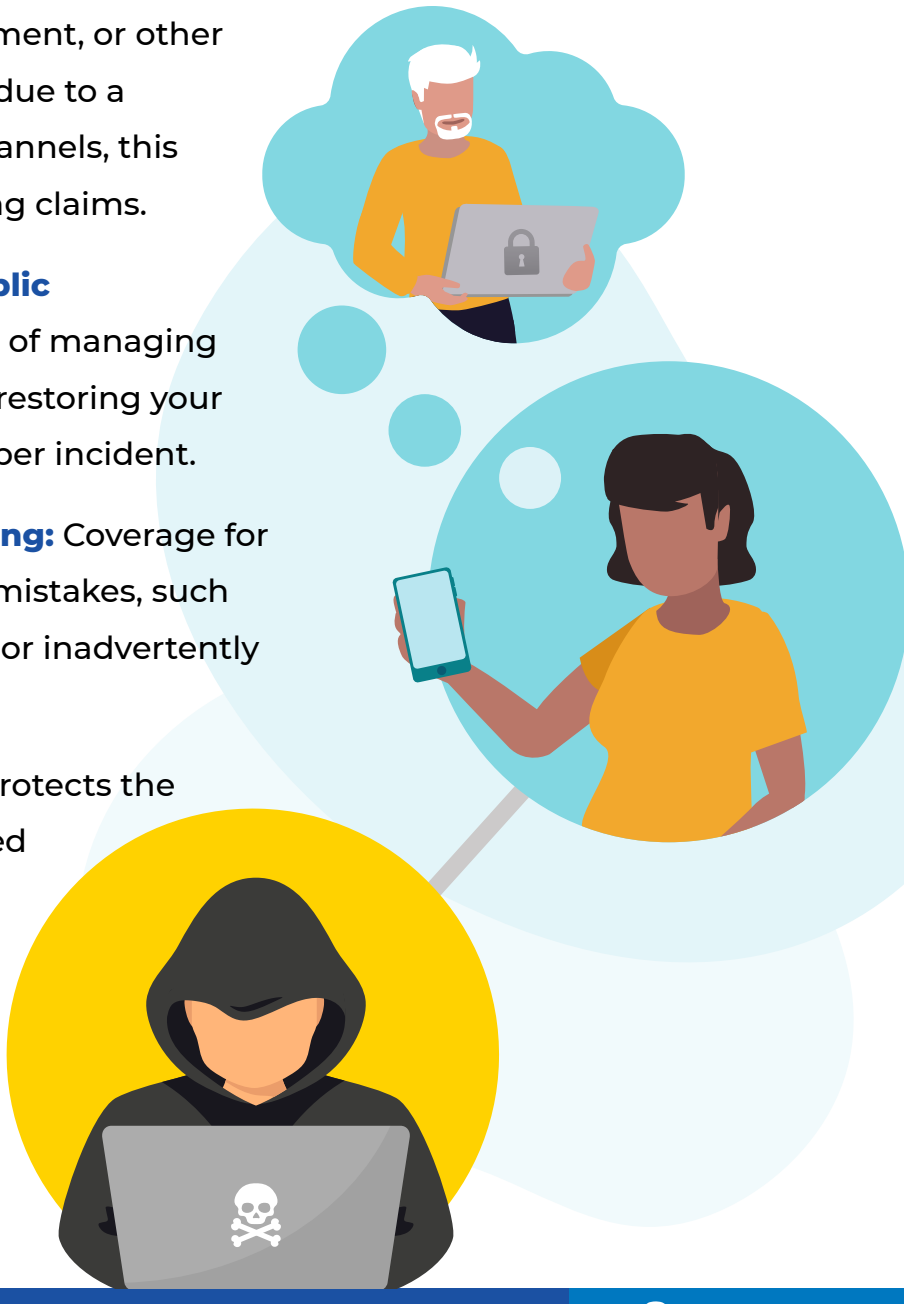
- **Network Security Liability:** Provides coverage for claims arising from the failure of your network security, such as viruses spreading to other systems or denial of service attacks on third-party networks.

- **Media Liability:** If a cyberattack leads to defamation, copyright infringement, or other intellectual property violations due to a breach of your digital media channels, this coverage addresses the resulting claims.

- **Crisis Management and Public Relations:** This covers the costs of managing the public relations fallout and restoring your business's reputation after a cyber incident.

- **Employee Errors and Phishing:** Coverage for incidents caused by employee mistakes, such as falling for phishing schemes or inadvertently causing a data breach.

- **Social Engineering Fraud:** Protects the business if employees are tricked into transferring money or confidential information to cybercriminals due to fraudulent communications.



- **Costs for System Restoration and Data Recovery:** Covers the expenses involved in restoring or repairing damaged IT systems and recovering lost or corrupted data after a cyberattack.
- **Coverage for Vendors/Third-Party Service Providers:** If your business relies on external vendors for critical services (like cloud storage or IT support), ensure the policy covers incidents involving these vendors.

By including these key elements in your comprehensive cybersecurity liability coverage, you will mitigate the financial and operational impact of any cyber incidents on your small business.

CHAPTER 3

How Banks Like Sonata Bank Help to Protect Small Businesses from Cyber Fraud

All banks have developed multiple protocols to outperform the bad actors and their cyber threats. These protective measures include the following:

Multi-Factor Authentication (MFA) – This added layer of MFA protection requires that a user provides multiple verification steps to access their accounts, which reduces the risk of their account being compromised.

Tokenization – Tokenization provides an added layer of protection for online and mobile banking platforms as well as the payment gateways because tokenization completely replaces your data with a token that cannot be reversed without access to the tokenization system. This prevents any unauthorized access to sensitive data.

Positive Pay – This fraud prevention tool matches checks presented for payment against the small business's authorized list of checks they have issued. If the check does not match, the bank flags it for review, alerts the small business and reduces the risk of fraudulent transactions.

Fraud Protection and Monitoring Systems – Banks use machine-learning algorithms to spot unauthorized transactions and suspicious activity, automatically freezing accounts to prevent further damage.

Incident Response and Recovery – We offer rapid recovery solutions in the event of a cyberattack, assisting with freezing accounts, recovering lost funds, working with law enforcement and supporting small businesses in the post-cyberattack protocols.

Account Controls and Alerts – Small businesses are granted the ability to set transaction limits, create automated alerts and employ dual-control systems where two people must authorize large transactions before they can go through.

Threat Intelligence Sharing – There are threat intelligence sharing networks, like Financial Services Information Sharing and Analysis Center (FS-ISAC). This sharing and receiving of data about cyber threats helps protect small business clients from emerging cyberattacks.

Routine Security Audits – Banks regularly check their systems and platforms for vulnerabilities, perform patch management and regular system updates.

A Dedicated Treasury Manager – At Sonata, our small business accounts have the option of working with a dedicated treasury manager who is an extra set of eyes watching their account, who is also identifying their opportunities for financial growth.

Thanks for Reading About Cyber Safety

We hope the insights and strategies we've shared here align with the steps you are already taking to protect your own small business from emerging cyber threats. By knowing the risks, best practices, and the right tools, your business will continue to stay secure in this increasingly complex digital world.

**You will be linking to another website not owned or operated by Sonata Bank. Sonata Bank is not responsible for the availability or content of this website and does not represent either the linked website or you, should you enter into a transaction. The inclusion of any hyperlink does not imply any endorsement, investigation, verification or monitoring by Sonata Bank of any information in any hyperlinked site. We encourage you to review their privacy and security policies which may differ from Sonata Bank.*