PRESENTER GUIDE

Department of Agriculture, Trade and Consumer Protection, Bureau of Consumer Protection

PRESENTATION: CYBERSECURITY FOR WISCONSIN BUSINESSES

The **Cybersecurity for Wisconsin Businesses presenter guide** is to be used in conjunction with the delivery of the presentation developed by the Bureau of Consumer Protection.

Audience: Non-technical business leaders, small-to-medium business (SMB) owners, and department heads. Business groups (chambers of commerce and rotary clubs).

Presentation Length: Approximately 60 – 75 minutes.

Purpose: This guide provides presenters with the resources needed to deliver the presentation effectively. It includes content, discussion prompts, talking points, and timed instructions for each slide, enabling flexible and adaptable delivery based on audience needs and time constraints.

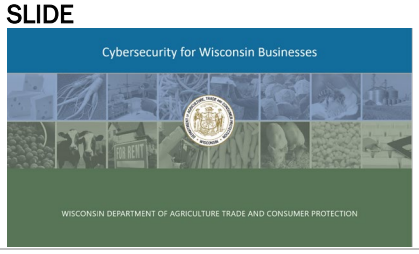
The guide is not intended for distribution among session participants.

TABLE OF CONTENT

1. Cover Page — 0.5 MIN

Facilitator Notes/Questions

SLIDE



2. Why We're Here — 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Use this slide to establish why cybersecurity is relevant to businesses of every size. Emphasize that cybersecurity is a business issue, not simply an IT issue.

NARRATIVE

- Cyberattacks are a risk for businesses of every size. Small businesses can be especially vulnerable because they may have fewer cybersecurity resources, less dedicated IT support, or fewer safeguards in place.
- At the same time, almost every business depends on technology in some way, whether that means email, online banking, customer information, payment systems, cloud services, or connected devices.
- The goal of cybersecurity is not to eliminate every possible risk. It is to take practical steps that reduce the likelihood of an attack and help the business respond and recover if something happens.

ADDITIONAL CONTEXT

- The slide emphasizes four introductory concepts: cyberattacks are increasing, every business can be targeted, small businesses may be particularly vulnerable, and prevention can cost less than recovering from an incident.
- If appropriate, ask participants to consider how their business would operate for a day without access to email, customer records, payment systems, or other essential technology.

RESOURCES

- **Fraud Against Business| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx

3. LEARNING OBJECTIVES

1 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Use this slide as a brief roadmap. There is no need to explain each topic in detail because each will be addressed later in the presentation.

NARRATIVE

- Today we will look at some of the most common cyber threats facing businesses, why businesses are targeted, and the financial and operational consequences an incident can have.
- More importantly, we'll focus on practical steps businesses and their employees can take to reduce risk, as well as what to do if a cybersecurity incident occurs.
- The emphasis throughout the presentation will be on practical actions businesses can take.

ADDITIONAL CONTEXT

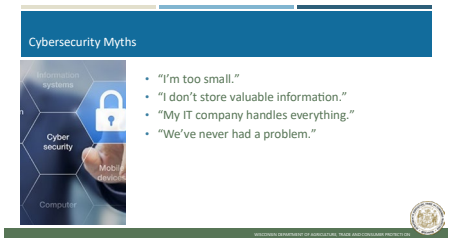
The presentation covers six primary areas: current cyber threats, why businesses are targeted, financial consequences, employee responsibilities, simple protections, and incident response.

4. CYBERSECURITY MYTHS

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Use the statements on the slide to challenge common assumptions about cybersecurity. Avoid spending significant time rebutting each statement individually; later slides provide additional context.

NARRATIVE

- Businesses sometimes underestimate their cybersecurity risk because they assume they are too small to be targeted or don't have information worth stealing.
- But criminals may be interested in much more than customer information. Business email accounts, banking information, employee information, passwords, and access to other organizations can all have value.
- Another common assumption is that an outside IT provider handles all cybersecurity responsibilities. IT support can be an important part of cybersecurity, but business owners and employees still play an important role—particularly in recognizing suspicious communications, protecting accounts, and following security procedures.
- Finally, never having experienced a known cybersecurity incident does not mean one cannot happen.

ADDITIONAL CONTEXT

If audience participation is appropriate, consider asking whether participants have heard any of these statements in their own workplaces.

RESOURCES

- **Privacy Protection Tips for Businesses| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx

5. THE MODERN CYBER THREAT | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Use this slide to introduce the range of cyber threats businesses may encounter. Keep the discussion at a high level; several of these threats will be addressed individually on the slides that follow.

NARRATIVE

- Cyber threats can take many forms. Some attacks are designed to steal money or information, while others attempt to gain access to business systems, disrupt operations, or trick employees into taking an action that benefits the criminal.
- These threats can also overlap. For example, a phishing email may be the first step in an attack that eventually leads to stolen information or ransomware.
- Over the next several slides, we will look more closely at some of the most common threats businesses should be prepared to recognize.

RESOURCES

- **Fraud Against Business| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx
- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

6. WHY CRIMINALS TARGET SMALL BUSINESSES | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Focus on why small businesses can be attractive targets for cybercriminals. Emphasize that being smaller does not mean a business has nothing of value to attackers.

NARRATIVE

- Small businesses may have fewer cybersecurity resources or limited IT support compared with larger organizations, but they still handle information and systems that criminals can use or monetize.
- That can include business bank accounts, customer information, employee information, passwords, payment information, and access to vendors or other organizations.
- Small businesses can also be targeted as a way to reach a larger organization. If a business is connected to a customer's, vendor's, or partner's systems, an attacker may try to use that relationship as another path into the larger network.
- The important takeaway is that cybercriminals are looking for opportunities, not just large companies.

ADDITIONAL CONTEXT

- Some cyberattacks use automated tools or Artificial Intelligence (A.I) to search for systems with known security weaknesses. This means a business may be targeted because a vulnerability is discovered, not because a criminal specifically selected that business.

RESOURCES

- **Privacy Protection Tips for Businesses| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx
- **NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide | U.S. Department of Commerce**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

7. WHAT DO THEY WANT? | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Help participants recognize the different types of information and assets that can have value to cybercriminals. Connect the examples on the slide to information businesses routinely use or maintain.

NARRATIVE

- When we think about cybercrime, we often think first about stealing money. Money and access to financial accounts are certainly important targets, but criminals may also be looking for information they can use, sell, or exploit.
- Customer and employee information can be valuable because it may contain personal or financial information that can be used for fraud or identity theft.
- Passwords and other login credentials can give criminals access to email accounts, financial systems, cloud services, or other business resources.
- Businesses may also possess intellectual property—such as designs, processes, business plans, proprietary information, or other materials—that has value.
- The key is to recognize what information and systems your business has that someone else might want.

RESOURCES

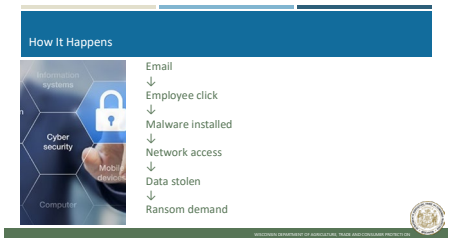
- **Identity Theft and Privacy Protection | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx
- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

8. How It Happens

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Walk participants through the sequence shown on the slide to demonstrate how one employee action can become the starting point for a larger cybersecurity incident. Explain that this is an example of how an attack can progress, not the sequence followed by every cyberattack.

NARRATIVE

- Let's look at one example of how a cyberattack can develop.
    - An employee receives an email that appears legitimate and clicks a malicious link or attachment. That action may allow malicious software to be installed or give the attacker access to an account or system.
    - Once inside, the attacker may try to gain additional access, move through the business's network, and locate valuable information.
    - Information may then be stolen, systems may be disrupted, or the business may receive a ransom demand.
- This is why something as simple as recognizing a suspicious email, and knowing what to do with it, can be an important part of protecting the entire business.
- Employee awareness and early detection are the strongest shields. If you can train your staff to pause and verify that first email, you cut off the attacker's path before they ever get near your data.

ADDITIONAL CONTEXT

- The sequence on the slide is intentionally simplified. Not every phishing attempt installs malware, not every successful intrusion results in ransomware, and attackers may gain access through other methods.

RESOURCES

- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

9. No Industry is Immune

1 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Use the examples on the slide to reinforce that cybersecurity risk is not limited to technology companies or large corporations. Connect the discussion to the types of businesses represented in the audience when possible.

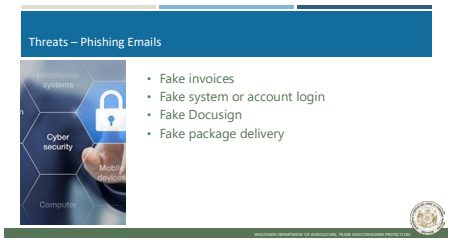
NARRATIVE

- Cyberattacks can affect organizations across virtually every industry.
  - Manufacturers rely on connected production systems.
  - Retailers depend on payment systems.
  - Farms increasingly use connected equipment and technology.
  - Law offices and medical clinics maintain sensitive information, while municipalities rely on digital systems to provide public services.
- The technology and information may differ from one organization to another, but every organization has systems, information, or operations worth protecting.

10. THREATS – PHISHING EMAILS | 2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTERS

Focus on helping participants recognize phishing as an attempt to get someone to click, provide information, or take another action. Emphasize the importance of pausing and verifying suspicious requests.

Consider using the following question to introduce the topic:

- Have you ever received an email that looked legitimate at first, but something about it made you question whether it was real?

NARRATIVE

- Phishing emails are designed to look legitimate so that the recipient will click a link, open an attachment, provide information, or take another action.
    - Common examples: A phishing message might appear to be an invoice, an account login notice, a Docusign or other electronic-signature request, or a package delivery notification.
- Encourage employees to slow down when a message is unexpected or creates a sense of urgency. Look carefully at the sender, links, attachments, and what the message is asking you to do.
- If something seems unusual, do not use the contact information or links provided in the message
- Verify the request separately using contact information you already know and trust.
- Phishing often succeeds by imitating familiar business activities and taking advantage of urgency or routine.

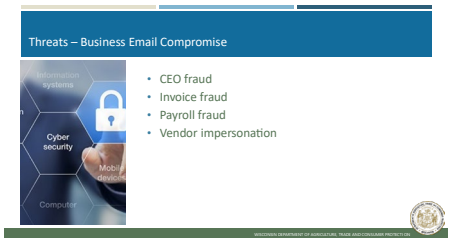
RESOURCES

- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

11. THREATS – BUSINESS EMAIL COMPROMISE | 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- Business email compromise (BEC) occurs when criminals use email to impersonate someone a business trusts—such as an owner, executive, employee, or vendor.
    - For example, an employee might receive what appears to be a message from the owner requesting a payment, or a vendor might appear to send new banking information for an upcoming invoice. Criminals may also impersonate employees to request changes to direct-deposit information.
- These messages can be convincing because they often look like normal business communications.
- Businesses should establish procedures for independently verifying requests involving payments, payroll changes, or banking information. A quick verification using a known phone number or another trusted communication method can prevent a costly mistake.

ADDITIONAL CONTEXT

- BEC may involve a spoofed email address or an actual email account that has been compromised. The technical method is less important than the prevention strategy: independently verify high-risk financial requests.

12. THREATS – RANSOMWARE

2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTERS

Focus on the business consequences of ransomware rather than the technical details of encryption. Connect locked data to the practical inability to conduct normal business operations.

NARRATIVE

- Ransomware is malicious software that can prevent a business from accessing its files or systems, often by encrypting them.
- The immediate problem is not simply losing access to a computer. A ransomware attack can interrupt scheduling, billing, payroll, production, customer service, and other essential operations.
- Attackers may demand payment in exchange for restoring access. In some cases, they may also steal information and threaten to release it.
- Recovery can require significant time and resources, including restoring business operations and addressing potential reputational damage. This is why prevention, backups, and an incident-response plan are so important.

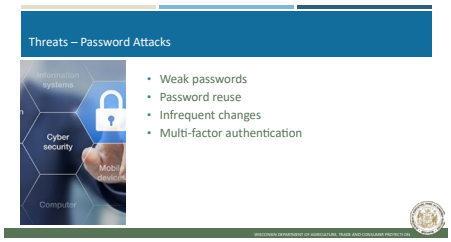
RESOURCES

- **Ransomware Prevention Guidelines | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/stopransomware

13. THREATS – PASSWORD ATTACKS | 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- Passwords are a common target: Criminals may try to gain access to business accounts by obtaining or guessing login credentials.
    - Note: Criminals can use stolen credentials and automated tools rather than manually guessing passwords.
- Weak passwords are easier to compromise: Short, common, or predictable passwords can make unauthorized access easier.
- Password reuse increases the risk: If a password is exposed through one account or data breach, criminals may try the same username and password on other accounts.
- Compromised passwords can provide broader access: A stolen password may give a criminal access to business email, financial accounts, cloud services, or other systems.
- A password alone may not be enough: If a criminal obtains a password, an account protected only by that password may be vulnerable. Use multifactor authenticator (MFA) when available.

RESOURCES

- **Secure Our World Password Best Practices Hub| Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/secure-our-world/use-strong-passwords
- **Multifactor Authentication Guide| Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication

14. THREATS – SOCIAL ENGINEERING | 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- Social engineering is when a criminal manipulates someone into providing information or taking an action they normally would not take.
- These attempts can happen through phone calls, text messages, email, or other communications.
    - For example, someone may pretend to be technical support and ask for access to a computer, or impersonate a vendor and claim that payment information needs to be changed immediately.
- These scams rely on manipulating people often through urgency, fear, trust, or authority—rather than defeating security technology.
- A common warning sign is pressure to act quickly.
- Employees should feel comfortable stopping, questioning an unusual request, and verifying it independently before taking action.

ADDITIONAL CONTEXT

- Terms such as vishing for voice phishing and smishing for text-message phishing may be useful background for presenters but do not need to be introduced unless they help the audience.

RESOURCES

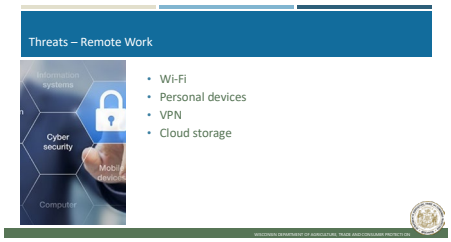
- **Social Engineering Awareness Portal | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

15. THREATS – REMOTE WORK

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTERS

Emphasize that business cybersecurity responsibilities extend beyond the physical workplace when employees work remotely. Focus on practical safeguards rather than technical network details. Consider using the following question to introduce the topic:

- What cybersecurity risks can arise when employees work outside the traditional workplace?

NARRATIVE

- **Wi-Fi:** Remote employees may use home or public networks that do not have the same protections as workplace networks. Home Wi-Fi should be secured, and employees should use caution when accessing business information over public Wi-Fi.
- **Personal devices:** Employees may use personal computers, phones, or tablets that the business does not manage. Businesses should establish clear rules about whether and how personal devices may be used for work.
- **VPN:** Remote connections to business systems can create another point of exposure. When appropriate, a virtual private network (VPN) can provide a more secure connection to business resources.
- **Cloud storage:** Remote employees may rely on cloud services to access or share files. Businesses should establish which services are approved and how business information may be stored and shared.

RESOURCES

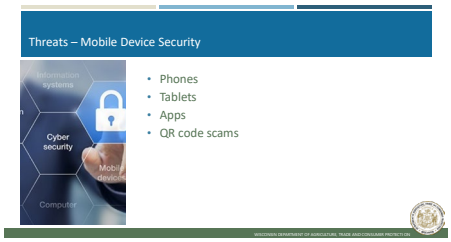
- **Secure Your Home Network Guide | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/news-events/news/securing-wireless-networks

16. THREATS – MOBILE DEVICE SECURITY

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Help participants recognize smartphones and tablets as business devices when they are used to access email, accounts, files, or other work information. Focus on simple security habits businesses can establish.

NARRATIVE

- Smartphones and tablets can contain or provide access to the same business information we protect on office computers—including email, accounts, documents, and customer information.
- Protect mobile devices with basic safeguards such as screen locks, strong authentication, and software updates.
- Employees should also be cautious about the apps they install and the links or QR codes they use.
- Because phones and tablets can easily be lost or stolen, businesses should establish a process for employees to report a missing device quickly so appropriate action can be taken.

ADDITIONAL CONTEXT

Depending on the size and needs of the business, mobile-device management tools may provide additional capabilities for managing business devices or protecting company information if a device is lost.

RESOURCES

- **Mobile Communications Best Practice Guidance | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance

17. THREATS – ARTIFICIAL INTELLIGENCE | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Focus on how artificial intelligence (A.I.) can make familiar scams more convincing rather than explaining the technology behind AI. Reinforce that established verification procedures remain effective even when a message, voice, or image appears authentic.

NARRATIVE

- Artificial intelligence (A.I.) can help criminals make existing scams more convincing. It can also help criminals create and carry out scams more quickly and on a larger scale.
    - For example, AI can help create professional-looking phishing messages, imitate someone's voice, or produce realistic fake images or videos.
- This makes it increasingly difficult to rely only on how a message looks or how a caller sounds when deciding whether a request is legitimate.
- If an employee receives an unusual or high-risk request—especially one involving money, account information, or sensitive business data—the safest response is to verify it independently using a trusted communication method.
- The technology may be changing, but the basic security practice remains the same: pause and verify before reacting.

RESOURCES

- **Artificial Intelligence Security Guidance Portal| Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/ai

18. Business Impact – Financial Costs

2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- The financial impact of a cyberattack can come from several directions.
- If systems are unavailable, a business may lose sales or revenue because customers cannot make purchases, schedule services, or complete transactions.
- Recovery can also create unexpected expenses, including IT assistance, restoring systems and data, legal or professional services, and other costs associated with responding to the incident.
- Downtime can be particularly costly because normal business expenses may continue even while the business is unable to operate normally.
- Cyber insurance may help with some costs, but coverage varies. Businesses should understand what their policy does and does not cover before an incident occurs.

RESOURCES

- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
- **Privacy Protection Tips for Businesses | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx

19. Business Impact – Reputation Damage

2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTERS

Focus on the relationship between cybersecurity and customer trust. The goal is to explain that reputational consequences can accompany financial and operational consequences.

NARRATIVE

- Trust is important to any business. Customers expect businesses to handle the personal and financial information they provide responsibly.
- When a cybersecurity incident exposes customer information or disrupts services, some customers may lose confidence in the business.
- An incident can also result in negative publicity, particularly if customers believe the business was unprepared or did not respond appropriately.
- Preparation matters. Having a response plan and communicating effectively when an incident occurs can help a business manage the situation and begin rebuilding trust.

RESOURCES

- **Cross-Sector Cybersecurity Performance Goals| Cybersecurity and Infrastructure Security Agency** https://www.cisa.gov/cross-sector-cybersecurity-performance-goals/cross-sector-cybersecurity-performance-goals

20. BUSINESS IMPACT – OPERATIONAL DISRUPTION

2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Use examples of everyday business operations that fit the audience, as every business does not have manufacturing or complex technology systems.

NARRATIVE

- Cyber incidents can prevent a business from carrying out basic operations.
- Depending on the business, that could mean production stops, employees cannot access payroll systems, orders cannot be shipped, or staff cannot access the information they need to assist customers.
- Even a business that does not rely on complex technology may depend on email, scheduling, accounting, payment processing, or customer records.
- Understanding which systems are essential to your business can help you plan how operations will continue or be restored following an incident.

RESOURCES

- **Privacy Protection Tips for Businesses | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx

21. LEGAL AND REGULATORY RESPONSIBILITIES | 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- Businesses may have legal, regulatory, and contractual responsibilities related to the information they maintain and how they respond to a cybersecurity incident. Requirements vary depending on the business, the information involved, applicable laws, and contractual obligations.
- **Data protection.** Businesses should understand what personal or sensitive information they maintain and what requirements may apply to protecting it.
- **Privacy:** Businesses should consider how personal information is collected, used, shared, stored, and disposed of, and understand the privacy requirements that may apply to their business.
- **Reporting requirements:** A cybersecurity or data breach may trigger notification or reporting requirements. In Wisconsin, state law establishes notification requirements in certain circumstances involving unauthorized acquisition of personal information.
- **Contracts:** Contracts with customers, vendors, insurers, or other business partners may also establish cybersecurity, privacy, data-protection, or incident-reporting responsibilities.
- **Know your responsibilities before an incident:** Understanding these responsibilities before an incident occurs can help a business respond appropriately and determine who may need to be contacted or notified.

ADDITIONAL CONTEXT

- **Wisconsin data breach notification law:** Wis. Stat. § 134.98 requires covered businesses operating in Wisconsin and maintaining specified personal information about Wisconsin residents to provide notification when that information is acquired by an unauthorized person, subject to exceptions in the law. When notification is required, it must occur within a reasonable time, not exceeding 45 days after learning of the unauthorized acquisition.
- **Privacy**: Privacy requirements can vary depending on the type of information and the business or industry involved. DATCP maintains information about Wisconsin and federal privacy laws that can help presenters identify additional requirements that may apply.

RESOURCES

- **Wisconsin's Data Breach Notification Law | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftDataBreach607.aspx
- **Wisconsin Privacy Laws| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/PrivacyLaws.aspx
- **Privacy Protection Tips for Businesses| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx

22. CYBER INSURANCE

2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- Cyber insurance is one component of managing cybersecurity risk, it is not as a substitute for security practices.
- Cyber insurance may help businesses manage some of the financial risks associated with a cybersecurity incident.
- However, policies vary considerably. Businesses should understand what their policy covers, what it excludes, and what requirements they must follow for coverage to apply.
    - For example, a policy may establish procedures for reporting an incident or require the business to contact the insurer before hiring certain response services.
- Businesses should review their coverage before an incident occurs and discuss questions about coverage with their insurance agent, broker, or insurer.
- Cyber insurance can support a cybersecurity strategy, but it does not replace good security practices.

RESOURCES

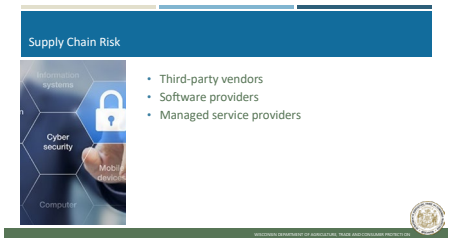
- **Consumer's Guide to Insurance for Small Business Owners | Wisconsin Office of the Commissioner of Insurance**
  https://oci.wi.gov/Documents/Consumers/PI-085.pdf
- **Tips for Buying Insurance Online| Wisconsin Office of the Commissioner of Insurance**
  https://oci.wi.gov/Pages/Consumers/PI-220.aspx

23. SUPPLY CHAIN RISK

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider using the following question to introduce the topic:

- What outside vendors or service providers have access to your business systems or information?

NARRATIVE

- Businesses routinely rely on outside organizations for services such as accounting, payroll, software, cloud storage, payment processing, and IT support.
- Those relationships can create cybersecurity risks because vendors may have access to business information or systems.
    - For example, a software provider could experience a security incident that affects its customers, or an outside IT provider could have credentials that provide access to a customer's systems.
- Businesses should understand which outside organizations have access to their information or systems and limit that access to what is actually needed.
- When a vendor relationship ends or access is no longer necessary, that access should be removed.

ADDITIONAL CONTEXT

- A managed service provider (MSP) is an outside company that manages technology or IT services for another business. If the term is unfamiliar to the audience, "outside IT provider" may be clearer.

RESOURCES

- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
- **Privacy Protection Tips for Businesses | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx

24. SECURE YOUR BUSINESS – FRAMEWORK | 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- Cybersecurity is not a one-time project. It is an ongoing process of understanding and managing risk.
- The NIST Cybersecurity Framework 2.0 provides businesses with a useful way to organize that process around six functions:
    - **Govern.** Establish how your business will manage cybersecurity risk, including responsibilities, policies, priorities, and expectations.
    - **Identify.** Understand the systems, information, equipment, and other assets your business needs to protect and the risks associated with them.
    - **Protect.** Put safeguards in place, such as strong passwords, multi-factor authentication, software updates, backups, and employee training.
    - **Detect.** Be prepared to recognize unusual activity or other signs that a cybersecurity incident may be occurring.
    - **Respond.** Know what actions to take and who to contact when an incident occurs.
    - **Recover.** Restore affected systems, information, and business operations following an incident.
- Businesses do not have to accomplish everything at once. The framework can help identify priorities and areas where cybersecurity practices can be strengthened.

ADDITIONAL CONTEXT

- NIST's Small Business Quick-Start Guide is specifically intended to help small and medium-sized businesses with modest or no existing cybersecurity plans begin managing cybersecurity risk.

RESOURCES

- **NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide | U.S. Department of Commerce**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

25. SECURE YOUR BUSINESS – PASSWORDS | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Focus on practical password practices rather than password-cracking terminology. Emphasize length, uniqueness, password managers, appropriate password changes, and multi-factor authentication.

NARRATIVE

- Strong passwords remain an important part of protecting business accounts.
- One approach is to use a long passphrase that is easier for you to remember but difficult for someone else to guess. For example, several unrelated words can create a long and strong passphrase.
    - A simple passphrase example could be:
        - Coffee-River-Bicycle-Window
        - The example demonstrates length and unrelated words; it should not be presented as a specific NIST-required format.
- Every important account should also have a unique password. Reusing the same password means that if one account is compromised, other accounts using that password may also be at risk.
- A password manager can help create and securely store unique passwords so employees do not have to remember every password themselves.
- Historically, organizations commonly required passwords to be changed every 30, 60, or 90 days. NIST provides updated guidance.
- Finally, use multi-factor authentication, or MFA, whenever it is available. MFA provides another layer of protection if a password is stolen.

RESOURCES

- **Secure Our World Password Best Practices Hub| Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/secure-our-world/use-strong-passwords

26. SECURE YOUR BUSINESS – EMPLOYEE TRAINING | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Consider using the following question to introduce the topic:

- Do your employees know what to do, and who to contact, if they receive a suspicious email or notice something unusual?

NARRATIVE

- Technology alone cannot prevent every cybersecurity incident. Employees also need to know what to look for and what to do when something seems wrong.
- Businesses should establish clear cybersecurity procedures and make sure employees understand their responsibilities if an incident occurs.
- Training helps employees recognize warning signs such as suspicious emails, unusual login requests, unexpected invoices, or urgent requests involving money or sensitive information.
    - Cybercriminals constantly refine their scams, but their core psychological tactics stay the same. Train staff to recognize unusual software pop-ups, strange bills, and urgent email requests.
- Businesses may also use phishing exercises or other training activities to help employees practice identifying suspicious messages.
- Most importantly, employees should know how and where to report something suspicious immediately. Early reporting gives the business more time to respond and limit potential damage.
    - Encourage a reporting environment in which employees can promptly report suspicious activity or mistakes. Fear of punishment may delay reporting at the exact time a business needs information quickly.

RESOURCES

- **Cybersecurity Training & Exercises | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-training-exercises

27. SECURE YOUR BUSINESS – SOFTWARE

2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- Software updates often include security fixes for weaknesses that have been discovered after the software was released.
- Delaying an update can leave a known weakness available for criminals to exploit.
- Enable automatic updates whenever possible so important security fixes are installed without depending on someone to remember to do it manually.
- Remember that updates are not limited to computers and phones. Routers, printers, and other connected devices may also contain software or firmware that needs to be updated.
- When you need technical assistance, use contact information from the software company, device manufacturer, or another trusted source rather than an unexpected pop-up or unverified support number.

RESOURCES

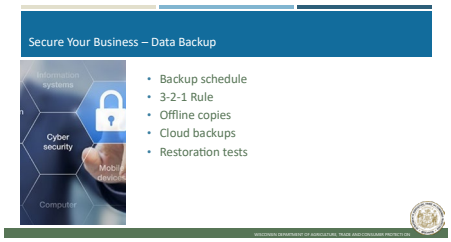
- **Cybersecurity Hygiene Services | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/cyber-hygiene-services
- **Cybersecurity Evaluation Tool and modules | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/sites/default/files/2024-03/23_0531_CISA_CSET_Factsheet_Final_508%20%281%29.pdf

28. SECURE YOUR BUSINESS – DATA BACKUP

3 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Emphasize that backups should be tested to make sure information can actually be restored.

NARRATIVE

- Backups help a business recover information if files are lost, damaged, or made inaccessible during a cybersecurity incident.
- A commonly used approach is the **3-2-1 backup rule**:
  - Keep three copies of important data—the working copy and two backups.
  - Keep those copies using two different types of storage.
  - Keep at least one copy separate from the primary business systems, so an incident affecting those systems does not also affect every backup.
- Cloud services can be part of a backup strategy, as can offline or otherwise separated backups.
- Whatever method you use, test your backups periodically. A backup is only useful if the business can successfully restore the information when it is needed.

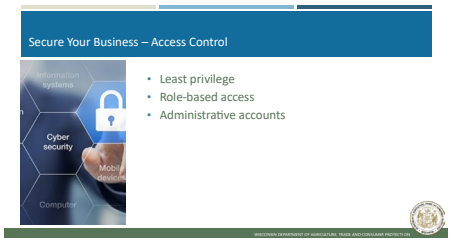
RESOURCES

- **Back Up Sensitive Business Information | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/back-up-business-data

29. SECURE YOUR BUSINESS – ACCESS CONTROL | 2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Access control is a simple principle: employees should have access only to the systems and information they need to perform their jobs.

NARRATIVE

- Not every employee needs access to every business system or file.
- A good security practice is to give employees access only to the information and systems necessary for their job responsibilities. This is sometimes called the **principle of least privilege**.
- Businesses can accomplish this by assigning access based on job roles.
- Administrative accounts deserve particular attention because they may allow someone to install software, change security settings, create accounts, or make other significant changes.
- Limit administrative access to people who genuinely need it, and remove access promptly when an employee changes roles or leaves the organization.
- Trust is a necessary community asset, "digital trust" must be tightly restricted.

RESOURCES

- **Identity and Access Management Recommended Best Practices Guide for Administrators | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management

30. SECURE YOUR BUSINESS – INCIDENT RESPONSE | 3 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Consider using the following question to introduce the topic:

- If your business experienced a cybersecurity incident today, would employees know what to do and who to contact?

NARRATIVE

- A cybersecurity incident is much easier to manage when the business has already decided what to do and who is responsible for doing it.
- An incident-response plan does not need to be complicated. It can begin with a step-by-step checklist that answers basic questions.
    - What systems and business functions need to be restored first?
    - Who needs to be contacted—such as IT support, management, the insurance carrier, legal counsel, or law enforcement when appropriate?
    - How will an affected device or system be isolated to help prevent the problem from spreading?
    - Who is responsible for determining whether the incident needs to be reported and whether customers or others need to be notified?
    - How will backups be accessed and business information restored?
- The plan should also address communication with vendors and, when appropriate, customers or the public.
- Most importantly, don't wait for an emergency to determine the answers. Write them down, assign responsibilities, and make sure the people involved know the plan.

ADDITIONAL CONTEXT

- "Public relations" does not necessarily mean hiring a public-relations firm. For a small business, it may simply mean deciding in advance who will communicate externally, what information can be shared, and how communications will be coordinated.

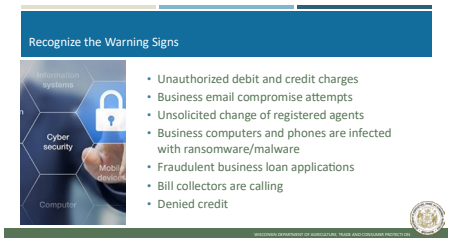
RESOURCES

- **Data Breaches| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx
- **Responding to a Cyber Incident | National Institute of Standards and Technology (NIST)**
  https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/responding-cyber-incident

31. RECOGNIZE THE WARNING SIGNS | 3 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Encourage participants to pay attention to unusual financial, account, and operational activity that may indicate fraud, identity theft, or unauthorized access.

NARRATIVE

- A cybersecurity incident is not always announced by a ransom message or a locked computer. Sometimes the first warning sign appears in a bank statement, credit report, email account, or business record.
- Watch for unauthorized debit or credit charges and unexpected business email compromise attempts, especially requests involving payments or account changes.
- Businesses should also pay attention to changes they did not authorize, such as a change to a registered agent, or signs that computers or phones may be infected with malware or ransomware.
- Other warning signs can include a lender contacting the business about a loan application it never submitted, calls from bill collectors about purchases the business did not make, or being denied credit for an account it never applied for.
- The important point is to investigate unexpected activity rather than assume it is simply an administrative error.

RESOURCES

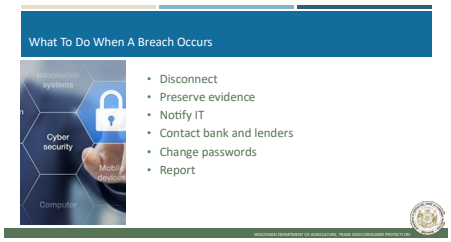
- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

32. WHAT TO DO WHEN A BREACH OCCURS

3 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

- Emphasize immediate, organized response rather than panic. Every incident does not require exactly the same technical response.

NARRATIVE

- If a cybersecurity incident occurs, the first priority is to contain the problem and prevent additional damage.
- Disconnect affected systems from the network when appropriate, but avoid immediately wiping, resetting, or rebuilding devices. Those systems may contain information that helps IT professionals or investigators determine what happened.
- Notify your IT provider or cybersecurity team and appropriate members of management.
- If financial accounts or payment information may be affected, contact your bank or other financial institutions promptly so they can help monitor or protect those accounts.
- After affected systems have been secured, change compromised passwords using a device you know is safe. Do not change passwords from a device that may still be infected.
- Preserve relevant records, logs, messages, and other evidence, and report the incident to the appropriate organizations or authorities based on the circumstances.
- The faster a business follows a prepared response plan, the better positioned it will be to contain the incident and begin recovery.

RESOURCES

- **Privacy Protection Tips for Businesses| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx
- **Data Breaches| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx
- **Data Breach Response: A Guide for Business| Federal Trade Commission**
  https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

33. RESOURCES FOR WISCONSIN BUSINESSES | 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- Businesses do not have to manage cybersecurity alone. Several state and federal agencies provide free guidance, tools, and reporting resources.
- DATCP provides Wisconsin businesses with information about privacy protection, business identity theft, and data breaches.
- The Federal Trade Commission offers cybersecurity guidance developed specifically for small businesses.
- If a business experiences cybercrime or online fraud, the FBI provides reporting through the Internet Crime Complaint Center, commonly known as IC3.
- Depending on the incident, businesses may also need to contact local law enforcement.
- The Cybersecurity and Infrastructure Security Agency, or CISA, provides cybersecurity best practices, tools, and technical resources.
- The Small Business Administration offers cybersecurity information and other resources for small-business owners.
- Bookmarking these specific resources before an emergency occurs gives an independent operation the exact same blueprint and reporting channels used by major

RESOURCES

- **Privacy Protection Tips for Businesses| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/IdentityTheftTipsBusiness.aspx
- **Cybersecurity for Small Business | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
- **Secure Your Business | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business
- **Strengthen your cybersecurity | U.S. Small Business Administration**
  https://www.sba.gov/counseling/manage-your-business/#strengthen-your-cybersecurity

34. LEARN MORE ABOUT DATCP — 1 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

- DATCP provides additional consumer-protection information through its website and social media channels.
- The Department also offers presentations on a variety of consumer-protection topics for community groups, organizations, and businesses across Wisconsin.
- Topics include scams and fraud, identity theft and privacy protection, landlord and tenant rights and responsibilities, safe online shopping, home improvement contracts, cryptocurrency, artificial intelligence, business identity theft, and other consumer-protection issues.
- Presentations may be available in person or virtually, and information about requesting a presentation is available through DATCP's website.

35. THANK YOU — 0.5 MIN

Facilitator Notes/Questions

SLIDE