Cybersecurity is critical to all businesses, especially small businesses. Continuing from our previous section, Cybersecurity Basics for Small Business, next we cover the various types of cyber attacks, means for protecting (cyber defense) your small business from cyber threats, and additional resources.

Cyber Attacks

Types of Cyber Attacks & Threats

There are a variety of ways in which cybercrimes are perpetuated. The following is a listing of

types of cybersecurity threats and their methods.

- Malware is a type of software used to perform an unauthorized function or process. This unauthorized software can perform actions such as tracking keystrokes and keyboard events (key logger), thereby enabling the theft of confidential information and passwords, for example.
- Ransomware is a type of malicious software designed to extort money by blocking access to files or the entire computer system until the ransom is paid. According to a report released by cybersecurity firm SonicWall, ransomware attack volume has increased by 185% in 2021. This is significant as the majority of businesses impacted by a ransomware attack suffer devastating financial losses.
- Phishing is the practice of sending fraudulent emails in order to obtain sensitive data. This is a form of social engineering used to trick an individual into disclosing confidential information about themselves This can include targeting employees in order to attain sensitive business information.
- Spyware is software that is secretly installed into an information system, often through fraudulent emails or websites. The software is then able to monitor all behavior that occurs on the infected computer, including things such as email usage, browsing behavior, and file access.
- A Virus is a type of program that replicates and infects a computer. Computer viruses are typically spread through infected email attachments, removable media (such as flash drives), and internet downloads.

For more information on these cyber attacks and threats, visit: What is Cybersecurity?

Reporting Cyber Attacks & Crimes

Inform law enforcement and the state attorney of any and all cyber attacks and crimes.

- Report stolen information to the Internet Crime Complaint Center (IC3).
- Report fraud to the Federal Trade Commission (FTC).
- Report Network Vulnerabilities to the United States Computer Emergency Readiness Team (US-CERT).
- Report any large cybercrimes to the Federal Bureau of Investigation (FBI).

In addition, most states maintain specific requirements for notification in the case of a security breach. These disclosure requirements are available here: Security Breach Notification Laws.

Cyber Defense Against Cyber Attacks

Cybersecurity defenses (or cyber defenses, for short), are proactive approaches to mitigate the risks of cyber attacks and threats. They focus on preventing, detecting and providing timely responses to cyber attacks or threats so that no infrastructure or information is tampered with.

Software

Installing protective software is one way to guard your information systems. Antivirus and

antispyware software can detect and eliminate malicious software that may be installed onto a computer. Firewalls prevent computers from outside your network from connecting and stealing shared data. Utilizing a WPA2 wireless network will ensure that only authorized users may access the Wi-Fi connection by requiring a secret password. Encryption software ensures that sensitive business information is unreadable to unauthorized users.

Examples: *Antivirus, Antispyware, Firewalls, Encryption, Trusted Platform Modules, SSID, IDPS, WPA2*

Procedural

Developing policies and procedures for your employees can help prevent unauthorized

access. These include instructing employees to develop complex passwords that are changed often and follow the Digital Identity Guidelines set forth by NIST. Other procedures include only providing them access to the systems and information they need, and preventing them from accessing fraudulent websites through web filters. Make sure that cybersecurity training is up-to-date and occurs on a regular basis.

Examples: *Multi-Factor Authentication, Limited Access, Email/Web Filters, Activity Logs, HTTPS/VPN*

Physical

Ensuring that your business and its devices are physically secure can prevent data theft that

will compromise your business. Locking computers after use and utilizing a physical lock which attaches the computer to a desk, can prevent an unauthorized person from taking the computer and extracting information. Privacy screens can also help prevent people from viewing confidential data.

Examples: *Drive Locks, Surge Protectors, Uninterruptable Power Supplies, Computer Locks, Privacy Screens*

More Information on Key Terms

For more information on these terms, visit: NIST Glossary

Considerations for Remote Work

In the light of the increased prevalence of remote work, cybersecurity practices must be

extended to include specialized protocols in dealing with telecommuting. Remote work has its own challenges for small business owners – cybersecurity risks are increased significantly when business information is remotely accessed.

Here are a few ways to help ensure the safety of your business information as remote work continues:

- Develop a cybersecurity policy specifically for telecommuting workers, in addition to your general cybersecurity policy.
- Use multi-factor authentication for access to remote work devices. This helps to prevent non-employees from accessing your business's information.
- Encryption of sensitive business information. How much and what is encrypted is up to you as the business owner, but options include encrypting a specific file or folder, volume encryption for multiple files or folders, and full-disk encryption which encrypts everything on the device automatically.
- If possible, provide company devices for your remote workers to work from. This allows for more control over the device's security: things like software installation, password protection, and file sharing can be better tracked and controlled.
- If employees are using their own devices, consider using a VPN and/or remote access desktop.

This list is not exhaustive. For more information, visit: NIST – Guide to Enterprise Telework, Remote Access, and BYOD Solutions

Additional

Take advantage of all the ways you can protect your business’ data. Purchasing cyber-

insurance can reimburse the value of any stolen data. However, in order to receive payouts, the business must implement and maintain an up-to-date cybersecurity program. Performing background checks on employees is also an important measure that can prevent malicious actors from stealing your information from inside the company.

For more examples of ways to protect your business from cyber attacks visit: NIST – Framework for Improving Critical Infrastructure Cybersecurity, FEMA – Be Prepared for a Cyberattack, FTC Protecting Personal Information, FTC Start With Security

Advanced Cyber Defenses

In additional to the measures listed above, there are several advanced tools you can use to protect your business:

- Next Generation Firewall (NGFW)
- Intrusion Prevention Systems (IPS)
- Deploy Demilitarized Zone (DMZ)
- Virtual Private Networking (VPN)
- Local Area Networks Layers (LAN)
- Digital Signatures (DSA, RSA, EDCSA)
- Encryption (AES, Triple DES)

For more information on what these advanced measures mean, visit: NIST Glossary

More on Cybersecurity for Small Businesses

To continue learning about Cybersecurity for Small Businesses, view the next sections:

- Cybersecurity Plans & Implementation for Small Business
- Cybersecurity & Government Contracting
- General Cybersecurity Resources & Contacts

Or return to Cybersecurity Basics for Small Business.

Additional Small Business Resources

Already in business or thinking about starting your own small business? Check out our various small business resources:

- View more business reports here: Small Business Snapshots
- View industry-specific research here: Market Research Links
- View small business help topics here: Small Business Information Center
- View business plans samples here: Sample Business Plans

Remember, you can also receive free professional business advice and free or low-cost business training from your local Small Business Development Center!