Cybersecurity is critical to all businesses, especially small businesses. Continuing from our previous section, Cyber Attacks & Defenses for Small Business, next we cover strategies and resources for developing and implementing cybersecurity plans, including frameworks, policies and related resources. While the following information is extensive, it should not be used as a substitute for consultation with a cybersecurity professional. Always consult IT professionals to ensure proper implementation of cybersecurity programs.

Cybersecurity Top Tips

There are several easy and immediate steps your business can take to better protect its sensitive information from cyberattacks.

1. Create Security Policies: Establish security practices and policies to protect sensitive information. Detail penalties for violating company cybersecurity policies.
2. Educate Employees: Establish rules of behavior describing how to handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating cybersecurity policies, and hold employees accountable.
3. Update Systems: Install antivirus and antispyware software to protect against viruses, spyware and other malicious code. Install key software patches and updates as soon as they are available.
4. Secure Networks: Safeguard your Internet connection with firewall security. Hide your

Wi-Fi network. Set up the wireless access point or router so that it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

5. Limit Access: Do not provide any one employee with access to all data systems. Only provide employees with access to the specific data systems that they need for their jobs. Do not enable employees to install any software without permission.
6. Use Complex Passwords: Require employees to use strong passwords and change them often. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry.
7. Secure Mobile Devices: 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.
8. Make Backups: Backup data automatically if possible, or at least weekly, and store the copies either offsite or in the cloud. Make copies of critical data such as word processing documents, electronic spreadsheets, databases, financial files, human resource files, and accounts receivable/payable files.
9. Protect Payment Cards: Work with banks to ensure the most trusted and validated tools and anti-fraud services are beings used for payment cards. Isolate payment systems from other, less secure programs. Don't use the same computer to process payments and surf the internet.
10. Control Physical Access: Lock computers when they are unintended. Create a separate user account for each employee. Only give administrative privileges to trusted IT staff and key personnel.

View the following resources for additional information: CISA – Small Business Resources, FTC – Secure Remote Access Tips, FCC – Ten Cybersecurity Tips for Small Businesses, Small Business Cybersecurity 101: Simple Tips To Protect Your Data

Cybersecurity Implementation

The following resources will take you step-by-step towards the path of implementing a comprehensive cybersecurity program. Each step is covered in detail by the National Institute for Standards and Technology (NIST) Publication *Small Business Information Security: The Fundamentals*, which serves as the industry framework.

I. Identify

- *Identify and control who has access to your business information.*
- *Conduct background checks.* Perform full nationwide, criminal background and sexual offender checks. If possible, perform a credit check on all prospective employers.
- *Require individual user accounts for each employee.* Require that complex passwords (16-string alphanumeric with special characters) be utilized for each account, and changed every 3–6 months.
- *Create policies and procedures for information security.* All employees should sign a statement agreeing that they have read the policies and relevant procedures and that they will comply with the policies and procedures.

View these tools to identify your vulnerabilities: FTC Start With Security, Test Your Knowledge, Delaware SBDC – Cyber Risk Assessment Tool

II. Protect

- *Limit employee access to data and information.*
- *Install Surge Protectors and Uninterruptible Power Supplies (UPS).* Surge protectors prevent variations in power from damaging electronic systems. Uninterruptible Power Supplies provide a limited amount of battery power to provide enough time to save data when the electricity goes off. Ensure all computers and critical network devices are plugged into a UPS. Plug less sensitive electronics into surge protectors.
- *Patch your operating systems and applications. Install and activate software and hardware firewalls on all your business network.*
- *Secure your wireless access points and networks.*

- *Set up web and email filters.* Email filters can help remove emails known to have malware attached. Consider blocking employees from going to websites that are frequently associated with cybersecurity threats. Many firewalls and routers can be set up to block certain addresses (blacklist), or allow only certain addresses (whitelist).
- *Use encryption for sensitive business information.* Use full-disk encryption, which encrypts all information on the storage media, on all computers, tablets, and smart phones.
- *Dispose of old computers and media safely.* Electronically wipe hard drives before disposing of old computers. After wiping the hard drive, remove it and have it physically destroyed. Install a remote-wiping application.
- *Train your employees.*

For more detailed information on implementing a cybersecurity plan visit: FTC Protecting Personal Information, FCC – Cybersecurity Planning Guide, FCC – Interactive Cybersecurity Planning Guide, NIST – Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security

III. Detect

- *Install and update anti-virus, anti-spyware, and other anti-malware software.*
- *Maintain and monitor logs.* Protection/detection hardware or software often has the capability of keeping a log of activity. Ensure this functionality is enabled. Logs can be used to identify suspicious activity and may be valuable in the case of an investigation. Logs should be backed up and saved for at least a year; some types of information may need to be stored for a minimum of six years.

IV. Respond

- *Develop a plan for disasters and information security incidents.* Determine who makes the decision to initiate recovery procedures and who will be the contact with the appropriate law enforcement personnel. Decide what to do with your information and information systems, including shutting down or locking computers, moving to a backup site, and physically removing important documents. Designate how and when to contact senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers or insurance providers, and the appropriate authorities.

For more detailed information on how to respond to a breach visit: FTC – Data Breach Response Guide, Experian – Data Breach Response Guide

V. Recover

- *Make full and incremental backups of important information.* The storage device should have enough capacity to hold data for 52 weekly backups. Periodically test your backed up data to ensure it can be read reliably. Consider encrypting backups to provide an added layer of security. Keep a copy of your encryption password or key in a secure location separate from where the backups are stored.
- *Consider cyber insurance.* Cyber insurance is similar to other types of insurance (e.g. flood, fire). Determine cyber security risks and research protection coverage offered by different policies.
- *Make improvements to processes, procedures and technologies.* Consider conducting

training or tabletop exercises, which simulate a major event scenario in order to identify potential weaknesses.

More on Cybersecurity for Small Businesses

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

- Cybersecurity & Government Contracting
- General Cybersecurity Resources & Contacts

Or return to Cybersecurity Basics for Small Business and Cyber Attacks & Defenses 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!