5 STEPS TO BETTER BUSINESS CYBERSECURITY GUIDE

Cybersecurity for your business is not only about adding layers of security technology. It starts with understanding and managing your cybersecurity risks. The 5 STEPS TO BETTER BUSINESS CYBERSECURITY, based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, represent an approach that applies to the specifics of your business, helping you understand how best to identify and protect your business's vital data and technology assets, and how to detect, respond to and recover from a cybersecurity incident.

IDENTIFY

Take inventory of key technologies you use and know what information you need to rebuild your infrastructure from scratch. Inventory the key data you use and store and keep track of likely threats.

- **Document assets.** Record the manufacturer, make, model, serial number, and support information for hardware and software. For software, know the specific version that is installed and running.
- **Determine location.** Locate all hardware devices attached to your network. They may be in your office, a data center, in the cloud or mobile.
- **Locate all key data.** Make sure you know in which software and on what devices it is stored or transmitted.

PROTECT

Assess what protective measures you need to have in place to be as prepared as possible for a cyber incident. Put protective policies in place for technologies, data and users, and ensure that your contracts with cloud and other technology service providers include the same protections.

Protective Measures:

- **Obtain support contracts.** All software and hardware should be covered for system failures. If possible, put contracts in place for security incident response as well. At a minimum, identify security vendors in advance.
- **Install security updates and patches.** Patch all software and devices at least monthly. Start with operating systems, browsers, Java, and document readers. Watch for breaking threats that require immediate action.
- **Backup systems and data.** Store at least one backup offline and off-site – physically or in the cloud. Know what needs to be kept and for how long. Replace all storage devices proactively (Typical hard drive life is 3-5 years depending on type).
- **Segment your network.** Not all devices need to be interconnected. Keep servers with direct access from the Internet, such as email and web servers, separated from the rest of your network. Restrict user access to servers. All Internet connections must have a firewall, even at home.
- **Mobile devices.** Use strong passwords and two-factor authentication (2FA) when available, and encrypt sensitive data.
- **Wifi.** Should be encrypted. Protect the router with a strong password.
- **Email.** Encrypt sensitive content. Use spam and malware filters to help block phishing and other attacks. Use 2FA when available.
- **Cloud services.** Ensure there is a commercial contract with vendor accepting security responsibility.
- **Payment card systems.** Isolate payment systems from other, less secure programs on a separate computer. Work with banks or processors to ensure trusted tools and anti-fraud services are being used.
- **Cyber Insurance.** Consider obtaining insurance to cover risks that are too expensive to protect against.

Protective Policies:

- **Limit employee access to data and systems.** Limit user access only to systems and data they need to perform their duties. Train employees in data sensitivity and appropriate access. Limit software installation permissions.
- **Passwords and authentication.** Require strong passwords. Prohibit reusing passwords across systems and sharing of passwords or accounts. Implement two-factor authentication (2FA) when available. Check with vendors that handle payment data and email to see if they offer 2FA for your account.
- **Remote Access.** Remote access to business assets should be encrypted and use 2FA. Remote computers must have appropriate security measures in place, including those provided by employees or contractors. Antivirus and firewall protections should be in place at a minimum.
- **Data Privacy.** Have a privacy policy and train employees about its meaning. Collect only the data you need and securely dispose of data as soon as the business need is met.

DETECT

Put measures in place to alert you about current or imminent threats to system integrity, or loss or compromise of data. Train your users to identify and speedily report threats or incidents.

- **Email.** Monitor messages blocked by email filters.
- **Network.** Monitor traffic in and out of your network, looking for suspicious patterns and errors.
- **Desktop.** Monitor antivirus messages. Monitor patch and update installation.
- **Storage.** Monitor disk health and utilization.
- **Users.** Train employees to know what incidents and attacks need to be reported, and encourage speedy reporting.

RESPOND

Make and practice an incidence response plan to contain an attack or incident and maintain business operations in the short term.

- **Utilize spares and backups,** while continuing to capture operational data.
- **Know how** to stop an attack, stop exfiltration of data, and collect forensic evidence.
- **Know who** to contact for advice—security incident response specialists and legal counsel.

RECOVER

Know what to do to return to normal business operations after an incident. Protect sensitive data and your business reputation over the long term.

- **Create a Disaster Recovery Plan**, including likely attack/failure/disaster scenarios. Identify who makes the call on activating the plan and who is responsible for executing the steps.
- **Know data breach notification requirements** for your state and state(s) where your customers reside. Federal requirements may also apply.

The 5-step approach follows guidance from the "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.0, National Institute of Standards and Technology, February 12, 2014.

For additional resources see:

- **http://www.bbb.org/cybersecurity**
- **http://stopthinkconnect.org/**
- **https://www.us-cert.gov/ccubedvp**