Cybersecurity Guide Checklist

In our digital age, cyber threats are everywhere, and no one is off the radar — not even the smallest of businesses. When cyber-attacks happen, it's more than just a technical headache, you can be held liable for wrongfully accessed data, and it can bleed your finances. Worse, it can make your customers lose faith in you. Can you afford to possibly lose your business? This Cybersecurity Checklist isn't just a bunch of steps; it's your battle plan for keeping your business safe and your customers' trust intact.

Securing your most vital resource - PEOPLE

- [ ] Help employees understand that criminals will target your organization.
- [ ] Remember that good customer service includes protecting data.
- [ ] Consider establishing an Acceptable Use Policy detailing your expectations about data, personal devices, and next steps if the employment relationship ends.

Secure Your IT

- [ ] Rapidly apply software patch updates to all business and personal devices.
- [ ] Provide each employee with the least access needed to do their work. When they leave employment, disable access rapidly.
- [ ] Be thoughtful about Wi-Fi registered to your business. If someone commits a crime using your connection, you could be visited by law enforcement.
- [ ] When disposing of an IT device, be sure the data it contains has been erased.

Criminals will interrupt your business and charge for access to your own computers.

- [ ] Back up important data. Working backups allow you to recover from a ransomware attack without paying criminals.
- [ ] Regularly purge electronic data that is no longer needed, as this reduces your exposure if hacked.
- [ ] Meet with your team to discuss offline work procedures to follow when IT outages eventually occur.

Cloud providers can simplify IT.

- [ ] Rather than purchasing IT equipment that is expensive and difficult to maintain, subscribe to reputable cloud providers to meet your needs.
- [ ] Adjust your cloud services based on seasonal capacity needs.
- [ ] Seek security commitments during the contracting process.
- [ ] Understand the benefits and risks of generative artificial intelligence (AI) services before allowing company data to be uploaded.

Social media management is critical to your brand reputation.

- ☐ Understand what has been posted about your organization and seek to correct errors.
- ☐ Ensure that you protect your official social media accounts with complex, long passphrases.
- ☐ Be sure that you can manage your social media accounts even if particular employees leave the organization.

Physical security matters too.

- ☐ Locked facilities, intrusion alarms, and cameras.
- ☐ Use locks to protect IT equipment and paper records from theft.
- ☐ Shred paper records before disposal.

Seek professional advice from an attorney or Cybersecurity expert.

- ☐ You may be required to comply with specific requirements based on your industry or contracts.
- ☐ Cyber insurance is available to help with the costs of incident response.
- ☐ Visit **PlanoChamber.org** and use our Business Directory to search for IT Professional Service Providers.

Strive for Resilience

- ☐ Cross train employees in case some become unavailable.
- ☐ Consider how remote work and paperless processes might enable operations to continue throughout a disruption.
- ☐ Establish reciprocal agreements with other organizations.

FIND A CYBERSECURITY EXPERT
Our Business Directory features trusted professionals who specialize in Cybersecurity, Visit **members.planochamber.org** or Scan the QR Codefor more info.

In Collaboration with **The University of Texas at Dallas**

PLANO CHAMBER OF COMMERCE