ziprisk

Cyber Security Awareness

Simplest Way To Protect Your Business

By: Ziprisk Team

2020

In this session you will learn:

1. **What is Cybersecurity** and Why it is important to invest in proactive protection against cyber attack.
2. **Key actionable steps** required to protecting your business
3. **Prepare your employees and company** to respond to a potential breach.

Are you prepared?

Small businesses are a favorite target of cyber criminals — **small business cyber attacks were up 424% in 2018-2019**

Cyber-Attacks Put **60% of Small Companies Out of Business within 6 months** - Don't Be Next

What is Cyber Security & Why it matters?

Cyber Security is used to describe a **set of practices, measures and/or actions you can take to protect information** from being attacked and stolen.

Inescapable Brand Damage

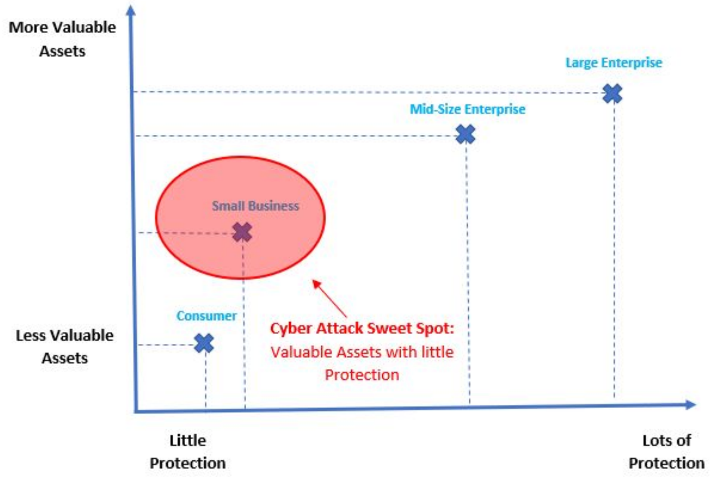
Investigations, Fines and Remediation

The average small business pays $36,000 to $50,000 for a Data Breach

Common Cyber Threats Include:

1. **Viruses, Malware, Ransomware** - encrypt/delete files, attack other computers, and make your computer run slowly.
2. **Phishing Attacks, Social Engineering** - sending fraudulent communications that appear to come from a reputable source (usually through email)
3. **Denial of Service Attacks (DoS) -** users are unable to access information systems, devices, or other network resources

ziprisk



SMBs typically spend less time and money on network security than larger firms.

That means they're easy targets for cyber criminals.

So what can you do?

Reduce the likelihood of Cyber Attacks by taking preventative measures

Cyber Security Plan of Action

1. Train your Employees on Cyber Security
2. Regularly update and patch your systems
3. Activate software firewalls and anti-virus solutions
4. Conduct a Risk Assessment every year
5. Keep a daily cloud backup of business data

T-R-A-C-K

Your

Plan of Action

Employee Awareness is the most important aspect of Cyber Security.

Most cyber breaches happen because an employee does something that he/she aren’t supposed to do.

Training Employees on Cyber Security Tips

1. **Be alert for phishing email** that requests them to open links or provide sensitive information. Do not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source.
2. **Avoid installing or downloading non-work related programs** onto the work computer. Unknown outside programs can open security vulnerabilities in networks.
3. **Ensure employees follow good password practices** by having a strong passwords and changing the password every 60-90 days.
4. **Encourage Employees to speak up** if they notice strange happenings on their computer.

THINK BEFORE YOU CLICK

CYBER SECURITY STARTS WITH YOU

Regularly update and patch your systems

1. **Software updates are important** because they often include critical patches to security holes.
2. **Malware attacks we see take advantage of software vulnerabilities** in common applications, like operating systems and browsers.
3. **Don't procrastinate software updates,** those updates are one of the most essential steps you can take when it comes to protecting your information.

Activate Firewalls and Anti-Virus Solutions

1. **Activating the latest security software (Firewall and Antivirus)** is one of the best defenses against viruses, malware, and other online threats.
2. **Firewall filters and blocks unwanted software**/malware from user-initiated Web/Internet traffic and prevents unauthorised access to or from a private computer network
3. **Anti-virus software scans and removes viruses** and malware from your systems

Conduct a Risk Assessment

A cybersecurity risk assessment identifies the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets.

1. **Identify Important Data:** What data is mission-critical to your business, and what are the systems that handle it?
2. **Identify Threats:** Who might want your data or wish to disrupt your operations? What are their capabilities and typical attack methods?
3. **Define Protection Standards:** Design security protocols that effectively handle your most valuable data and defend you against probable attacks

Keep a daily Cloud Backup of Business Data

Regular backups protect against the risk of damage or loss due to hardware failure, software or media faults, viruses or hacking, power failure, or even human errors.

1. **Protecting you in the event of hardware failure,** accidental deletions or disaster;
2. **Protecting you against unauthorised changes** made by an intruder;
3. **Providing you with a history of an intruder's activities** by looking through archived, older backups.

T-R-A-C-K Your Plan of Action

Sign up for our **FREE** employee onboarding & awareness at **www.ziprisk.com** and start protecting your business instantly!

About Ziprisk

We combine advanced Cyber Security and Ransomware Protection with Employee On-boarding and Awareness to defend your business against emerging HR and Cyber risks.

Our multi-layered cyber security solution is the simplest and most secure way for small businesses to protect their business data and employees.

Asian American Chamber of Commerce
of Greater Philadelphia
Making connections that matter...

AFRICAN-AMERICAN
CHAMBER OF COMMERCE
Pennsylvania ◆ New Jersey ◆ Delaware

GREATER PHILADELPHIA
HISPANIC CHAMBER
OF COMMERCE

ziprisk

Contact: 215-402-7900

www.ziprisk.com