Data Defense:
Creating a Robust Cyber Awareness Plan to Protect Your Company

Your data is one of your most valuable assets.

Welcome to the brave new world of cyber theft. Today's hackers are not only IT savvy, they're also savvy business people. Cybercrime is their full-time job, and their business model is finding new ways to attack yours. Sometimes they penetrate your systems and wait for months before they strike.

Cybersecurity isn't just an IT issue. It's a business issue. And the cost of prevention is minimal compared to the cost of recovering from a cyber fraud event.

Experts expect cybercrimes to cost the world $10.5 trillion annually by 2025.[1]

Every business needs a Cyber Awareness Plan.

How can you plan ahead? Like any security issue, you need multiple levels of mitigation.

At home, your doors may have a bolt lock, a chain, and an electronic alarm system — three layers of protection. A burglar will skip your house and go where the back door is unlocked.

The same principle holds true for your business: the more levels of mitigation you prepare, the more likely a cybercriminal will look elsewhere.

Start by forming your own Cyber Awareness advisory council of key players:

Information Technology, to make sure you have:

- an off-site, segregated network for your intellectual property and financial information;
- a systematic process to back up files to that site;
- and a protocol for changing passwords regularly (keeping them somewhere safer than a desk drawer).

continue >

Accounting, to help review your internal controls and safeguards, especially determining who has — and needs — access to your banking and other important records.

Insurance, to provide liability coverage for a breach — not to mention business interruption costs and recovery fees.

Legal, to make sure you report the attack according to disclosure laws.

Public Relations, to be ready with an action plan to manage the blow to your business' reputation.

Finance, to know your plan and how it can dovetail with the fraud protection services used by your company.

You'll also want to ensure that your bank offers a positive pay service. It enables the bank to compare the checks you write against the data in its system. Most banks offer a form of check and ACH Positive Pay services.

The time to bring your team together is now — before an attack.

A successful Cyber Awareness Plan requires training, refresher courses, and regular drills to keep employees up to speed on emerging threats. If a data breach occurs, having a well thought out incident response plan, that has been practiced and tested, is crucial to getting your business back to normal faster.

The fact is, cybersecurity isn't something you delegate. You're the one in charge — and the one who'll deal with the backlash from a data breach. The good news is, you don't have to face the problem alone: With trained staff and resources, you can take steps now to make your business more secure from now on.

Received a fraudulent or suspicious email that appears to be from Webster Bank?

Contact a Webster Relationship Manager or call 888-932-2256.

Want more information on protecting your company from cyber threats?
Connect with Webster Bank.

[1] Source: Cybersecurity Almanac, 2022.

COM-WP 0923