creativetechtalk
creativetechs.biz
June 2018

If you think your company is safe from cyber attack, think again.

It sent shockwaves throughout the business world: Equifax, one of the three largest credit-reporting agencies responsible for managing millions of consumers' credit data, announced last September that they had been hacked. Sensitive personal information for over 140 million U.S. customers was suspected of being compromised. Big businesses are not the only victims of cyber crimes like this, and the statistics relating to these crimes are chilling:

- *40% of all malicious attacks target small to medium-size businesses (SMBs).*
- *Approximately 50% of all SMBs have experienced an attempted data breach within the last year.*
- *60% of all SMBs that experience a successful cyber attack are unable to survive the first six months following the event.*

Welcome to the Dark Web

The term "Dark Web" sounds like something lurking in the shadows of a fictional spy novel, however, it is far from fictional. It's a place on the Internet where illegally acquired data is bought and sold. Customer, employee, and vendor data, as well as business information, e.g., trade secrets, client lists, and strategic marketing plans, are like gold for the hacker.

No One is Immune to Attack

Some of the most highly targeted business sectors include:

- *Construction and manufacturing*
- *Professional and legal services*
- *Financial institutions*
- *Non-profits*
- *Healthcare*
- *Real estate*
- *Educational institutions*
- *Architectural and design firms*
- *Government agencies*
- *Travel and transportation firms*
- *Retail and consumer-products companies*
- *Utility companies*

The Reality of Risk to Your Company

If your company has experienced a data breach, then you know fear is warranted; if you haven't, it's not a matter of *if* an attack will occur but rather *when*. Cyber Security is no longer optional. In today's business environment where digitization and mobility are increasingly necessary, the more digital and mobile we become, the more vulnerable we are to cyber attacks.

Continued on next page.

Watch the FREE WEBINAR

A Business Owner's Reasonable Response to CyberSecurity

Special Guest
Joshua Burkhardt

Beers, Miller, Backs, & Salin, LLP,
Attorneys at Law,
Fort Wayne, Indiana

AN EXPERT PANEL DISCUSSION COVERING:

- Can a breach happen to my company?
- What are the risks resulting from a cyber breach?
- How can I avoid a cyber attack?
- What is a reasonable response to cyber security?
- What should I do if I'm hacked?

Enter this URL in your browser window:

https://goo.gl/4WpDnp

or scan this QR code below to watch the video on your mobile device.

ctsi
creativetechnologysolutions inc

The vast majority of cyber attacks are the result of human error. These security breaches include:

- ***Phishing attacks*** *resulting from opening a fake email or visiting a harmful website;*
- ***Password theft*** *resulting from the use of weak passwords or passwords that are also used for personal accounts;*
- ***Ransomeware****, where a company's data are held hostage through encryption until a ransom, often equaling thousands of dollars, is paid;*
- ***Other Point-of-Entry attacks****, such as mobile devices and the use of unsecured WI-Fi networks.*

The Cost to Your Company

The harsh reality of a data breach is that while your company is a victim of a criminal act, ***it may also be held liable for damages incurred by your customers.*** Your legal responsibility to protect your data extends beyond your computer. It also includes other data formats, e.g., paper copies, and microfilm, even if the information has been transferred and is no longer stored on your computer.

In the event of a serious data breach, a company can typically expect tangible costs ranging from tens of thousands to hundreds of thousands of dollars. These costs cover a variety of necessary services, including:

- *Investigative services to verify the existence, nature, and scope of the breach;*
- *Corrective measures to halt the breach;*
- *Recovery services to restore your data and systems, and to prevent the breach from recurring;*
- *Legal services to protect your company from resulting litigation.*

There may be additional costs as well, both tangible and intangible, including:

- *Possible civil judgments and fines;*
- *Immediate and long-term loss of sales;*
- *Loss of employee productivity;*
- *Loss of customer trust and loyalty;*
- *Long-term damage to your brand value and market position.*

Virus Protection Isn't Enough

According the FBI's most recently released Cyber Crime briefing, the number of reported cyber attacks against businesses is expected to rise in coming years. Hackers are constantly adapting and changing their tactics. ***This requires a multi-vector strategy to data security that addresses all access points.*** In addition, your technology users need to be adequately trained to avoid making very costly mistakes.

If cyber security hasn't been on your radar, it should be. ***There is a reasonable approach to cyber security that can free you to focus on your business, while still providing peace of mind.***

Preparation & Prevention: Keys to your company's survival

Prevent and prepare now.

1. Take cyber security seriously.

Do not underestimate the value of your business data and the cost of replacing it! Protecting it should be a high priority, and a commitment to do so should be integrated at every level of your company's culture. Effective employee training is a must.

2. Know your company's risks.

- Have CTSi identify potential vulnerabilities in your data, network, storage devices, hardware and software, mobile devices, etc. You may also want to consider a broader compliance inventory that also evaluates the management of physical forms of your data.

- Know the potential recovery costs for your company should a breach occur. This will help you better understand the extent of your risks. Getting this estimation is easy with CTSi's free "Recovery-Time Calculator" at **www.creativetechs.biz/rtc.**

- Discuss your legal risk with an attorney who is experienced in cyber security law, and become familiar with your obligations in the event of a data breach.

- Discuss with your insurance agent whether your current business policy covers cyber attacks. You may be surprised to learn that you need a supplemental policy as well as a sound compliance plan to ensure payment in the event of a claim.

3. Develop a Data Incident Response Plan before your company needs it.

It's much better to have this developed ahead of time rather than wait until the heat of the battle. Your plan needs to identify all legal obligations, and it should prioritize all activities to ensure maximum compliance. It should also define your Data Incident Response Team, as well as outline expectations, roles, and responsibilities for each team member.

4. Put preventive measures in place.

Hackers never rest. So even if you have previously implemented preventive cyber security measures, you must remain vigilant. Adding a **Multi-Vector Strategy** to your cyber security program—one that addresses all access points—is the best way to anticipate, detect, and cut off hackers. CTSi can work with you to develop this strategy. **Technology alone, however, is not enough. The weakest link in any security program is the human element, and hackers know this. An effective security plan must also include comprehensive employee training.**

5. Keep your customer relations positive and strong.

A data event can result in an enormous public relations crisis for your company. Anything you can do now to maximize trust between you and your customers is like saving money in the bank for a rainy day.