1991 – 2021
30
YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

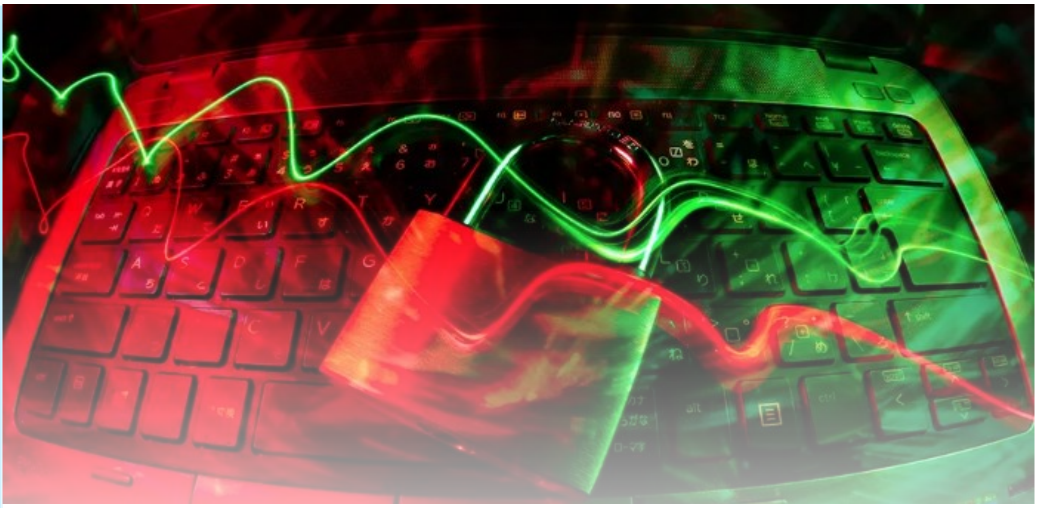
"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

November 2023

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"



It's Time to Get Serious About Cyber-Compliance

Introduction

Cyber compliance is the process of ensuring that organizations adhere to laws, regulations, and standards related to the use of technology. It is an essential part of any organization's security strategy as it helps protect against cyber threats and data breaches!

If that's not a compelling enough reason, you could also be held liable in an audit if you are caught slacking on cybersecurity.

Why Does Cyber Compliance Matter?

Organizations must employ a comprehensive cyber compliance program to ensure they are meeting all applicable laws and regulations. This program should include policies and procedures for identifying, managing, and responding to cyber threats as well as training employees on how to properly handle sensitive information. Creating this type of incident response plan will not only satisfy compliance regulations, but also cut down on the time it takes to report and respond to threats when they occur in real life!

Compliance laws aren't here to wrap you up in red tape. They're meant to better protect your personally identifiable information (commonly known as PII) as well as anyone else's protected data entrusted to your company's care, and yours as a consequence.

Continued on pg.2

Continued from pg.1

What Does Cyber Compliance Look Like?

Cyber compliance ensures that an organization's systems and data are secure from cyber threats. What does this involve?

- ***Assessing risks***
- ***Developing policies and procedures***
- ***Implementing security controls***
- ***Monitoring changes in technology***

These are just a few responsibilities involved. Organizations must ensure that their cyber compliance efforts are up to date in order to protect against the ever-evolving landscape of cyber threats. Cyber compliance is also essential for organizations that handle sensitive data, such as health records or financial information, as they must adhere to industry regulations in order to remain compliant.

By taking necessary steps to protect their systems and data, organizations can reduce the risk of breaches or other malicious activities!

Conclusion

Cyber compliance is not just mandatory; it's smart. It will ensure your cybersecurity posture is the most up-to-date and effective for your particular line of work, with trainings tailored down to your specific role in the organization depending on what kind of confidential data you handle! Healthcare workers, people working in finance, government workers and legal experts all have their own expectations and regulations when it comes to data privacy. The same is probably true for your job!

These days, you're pretty much guaranteed to encounter a cyberattack. If they successfully leak or steal data, and an audit finds that the company was lapsing in effective and mandatory security measures, then you could be held liable. This may comprise financial liability, recuperation fees, legal counsel, and lots of lost productivity!

The National Cybersecurity Alliance found that **two-thirds of SMBs go under within six months of a successful data breach**. Maintaining proper security awareness isn't just good for your data, but it's good for your job security too!

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

PROTECT YOUR NETWORK
"What Every Business Owner Must Know About Protecting and Preserving Their Network"
Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata1123/
or call our office at (248) 362-3800

Security Corner

Typosquatting: Your Guide to Understanding this Cyber-Threat

Typos or Fat fingers" are responsible for writing "teh" instead of "the" and accidentally ending a sentence in "1" instead of "!". Unlike a simple typo when you're messaging your friends, *typosquatting* is much more sinister.

What is Typosquatting?

It's known as URL hijacking, sting sites, and fake URLs. Also commonly referred to as typosquatting, this practice is when cybercriminals take common spelling errors of a legitimate website to entrap would-be users into giving out private info. For example…
They might send you to g00gle.com instead of the real search engine; of course, real typosquatters tend to be a little more clever and unnoticeable.

Typosquatting might use something like:

- A common misspelling
- A likely misspelling

Pluralizing a singular or vice versa
The typosquatter could then use this site to trick users into giving up their personal information or downloading malware.
So how can you protect yourself from typosquatting?

- Be careful when typing website addresses.
- Use a password manager to create and store strong passwords

Be wary of emails or pop-ups that ask for your personal information.
This is just one of many, many threats lurking out in the world wide web. Human error is responsible for 95% of cyber-attacks, including those that start with a very small typo.

For more information about typosquatting, call us at 248-362-3800 or visit: https://tinyurl.com/2p5z7v6e

Watch Out for Ransomware Pretending To Be a Windows Update

Imagine you're working away on your PC and see a Windows update prompt. Instead of ignoring it, you take action. But when you install what you think is a legitimate update, you're actually infected with ransomware.

Cybercriminals are constantly devising new ways to infiltrate systems. They encrypt valuable data, leaving victims with difficult choices. One such variant that has emerged recently is the "Big Head" ransomware.

The Big Head Ransomware Deception.

Big Head ransomware presents victims with a convincing and fake Windows update alert. Attackers design this fake alert to trick users. They think that their computer is undergoing a legitimate Windows update. The message may appear in a pop-up window or as a notification. The deception goes even further. The ransomware uses a forged Microsoft digital signature. The attack fools the victim into thinking it's a legitimate Windows update. They then unknowingly download and execute the ransomware onto their system. From there, the ransomware proceeds to encrypt the victim's files. Victims see a message demanding a ransom payment in exchange for the decryption key. Here are some strategies to safeguard yourself from ransomware attacks like Big Head:

Keep Software and Systems Updated

Big Head ransomware leverages the appearance of Windows updates. One way to be sure you're installing a real update is to automate. Verify the Authenticity of Update Genuine Windows updates will come directly from Microsoft's official website or through your IT service provider or Windows Update settings.

Backup Your Data
Regularly back up your important files. Use an external storage device or a secure cloud backup service. Backups of your data can allow you to restore your files without paying a ransom.

Use Robust Security Software

Install reputable antivirus and anti-malware software on your computer.

Use Email Security Measures

Put in place robust email security measures. Be cautious about opening email attachments or clicking on links.

Enable Firewall and Network Security

Activate your computer's firewall. Use network security solutions to prevent unauthorized access to your network and devices.

Disable Auto-Run Features
Configure your computer to automatically disable auto-run functionality for any external drives.

Be Wary of Pop-Up Alerts

Exercise caution when encountering pop-up alerts especially those that ask you to download or install software. Verify the legitimacy of such alerts before taking any action.

Keep an Eye on Your System

Keep an eye on your computer's performance and any unusual activity. If you notice anything suspicious, investigate immediately.

Have a Response Plan

In the unfortunate event of a ransomware attack, have a response plan in place. Know how to disconnect from the network. Report the incident to your IT department or a cybersecurity professional. Avoid paying the ransom if possible

5 Biggest Cybersecurity Mistakes of Small Companies

Cybercriminals can launch very sophisticated attacks. But it's often lax cybersecurity practices that enable most breaches and cyber incidents.

Small business owners often don't prioritize cybersecurity measures. They may be just trying to stay fully focused on growing the company.

Below are some of the biggest reasons small businesses fall victim to cyberattacks.

1. Underestimating the threat
2. Neglecting employee training
3. Using weak passwords
4. Ignoring software updates
5. Lacking a data backup plan

Secure By Design Cybersecurity Practices

Cybersecurity has become a critical foundation upon which many aspects of business rely. The frequency and sophistication of cyberattacks continue to increase. It's essential to shift from a reactive to a proactive cybersecurity approach, such as "**Secure by Design**."

Secure by Design integrates security measures into the very foundation of a system, app, or device. It does this from the start. It's about considering security as a fundamental aspect of the development process.

Key principles of Secure by Design include:
- Risk Assessment
- Standard Framework
- Least Privilege
- Defense in Depth
- Regular Updates
- User Education

Why Secure-by-Design Matters?
- Proactive Security
- Cost Savings
- Regulatory Compliance
- Reputation Management
- Future-Proofing
- Minimizing Attack Surfaces

Sustainable Tech Habits That Are A Win For Your Bottom Line

Below are several sustainable tech habits you can adopt:
- Energy-efficient hardware and appliances
- Virtualization and cloud computing
- Remote work and telecommuting
- Renewable energy sources
- E-waste recycling programs
- Paperless office
- Eco-friendly office supplies
- Software optimization
- Green IT certification
- Employee education and engagement
- Supply chain sustainability
- Lifecycle assessments

"A hacker logged into my fitness tracker and stole all my steps!"