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

October 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!"

Why Radio Silence Is The Wrong Response To A Cyber Event

Introduction

Have you ever had personally identifiable information (PII) exposed in a data breach? Whether it was your own or somebody else's, cyber events like this are increasingly common nowadays. In fact, **422M people had their information exposed in 2022.**

Depending on what you do for work, you may be responsible for protecting the private data of all sorts of people, from fellow coworkers to clients to government organizations with whom you do business! Couple that with the fact that ***95% of data breaches are borne of human error***, and you start to see that it's a matter of *if* and not *when* you will be compromised in a breach.

Why Trust & Transparency Matters

Transparency and communication are key when in the middle of a cyber-event, especially one that impacts others' PII on top of your own.

Think about it: the most important aspect of customer loyalty is TRUST. When you agree to let a company track your cookies, you expect them not to share that data with random people. If you tell something to your doctor or attorney, you expect them to keep it secret. Were any individual or company to break that trust, you would probably stop using their

Continued on pg.2

Continued from pg.1

services. In today's digital age, it's even common to blast them on social media!

The same basic concept is true when you experience a breach that affects other people's data. They want to know how it happened, what you're doing to fix it, and what steps you're taking to prevent it from happening again.

There are certain laws that may apply to you as well, which could dictate what you have to tell affected parties in a data breach. For example, banks must report significant attacks within 36 hours. Familiarize yourself with the regulations that apply to you!

The Solution is Simple

The best way to foster trust, even through an emergency, is ***honesty and communication***. Walk those who were affected through what's going on, so that they feel confident you're handling their data with as much care as possible.

Let's say you work in telecommunications, an industry that's been facing a barrage of cyberattacks lately. If your company's database was breached, you might send out a mass communication to anyone who was potentially affected, telling them things like…

- how many people's information was exposed
- what information was compromised; like names, account numbers, email addresses, etc.
- what steps the company is taking to mitigate the damage, like cooperating with authorities and reimbursing stolen fund
- how you plan to prevent this type of attack from happening again

Of course, don't do anything without the permission of your bosses, IT team and the authorities first!

Conclusion

Over half of businesses were involved in cyberattacks last year. SMBs have found themselves the target of such attacks increasingly often. If the same happens to you, don't keep it secret. Transparency, especially through hard times, fosters the best long-term relationships and customer loyalty.

It's not always our fault when information is exposed. Another insider or outsider threat could be behind a breach; what matters is keeping calm and remembering that the affected parties are looking to YOU as the gatekeeper of their privacy!

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!

SECURE OUR WORLD

CYBERSECURITY AWARENESS MONTH

Follow these top tips to stay safe online!

USE STRONG PASSWORDS...

Make your passwords:
Long: At least 16 characters
Complex: Use upper and lowercase letters, numbers and symbols
Unique: Use a different password for each account

...AND A PASSWORD MANAGER

Password managers can

- Store all your passwords
- Tell you when you have weak or re-used passwords
- Generate strong passwords for you
- Automatically fill logins into sites and apps

TURN ON MULTIFACTOR AUTHENTICATION

It provides **extra security** by confirming your identity when logging into accounts, like entering a code texted to a phone or generated by an authenticator app.

RECOGNIZE AND REPORT PHISHING

Common signs of a phish include:

- Urgent/alarming language
- Requests for personal or financial info
- Poor writing or misspellings
- Incorrect email addresses or links

Spot a phish? Report it, then delete it

UPDATE YOUR SOFTWARE

Software updates ensure your devices are protected against the latest threats. Turn on the **automatic updates** in your device's or app's security settings!

Security Corner

Are Cookies Taking A Bite Out of Your Data Privacy?

Have you heard of cookies before? No, not the kind made with chocolate chips or oatmeal raisins…

We're talking about Internet cookies. These cookies are small text files that websites save on your computer or mobile device when you visit them. They are used to remember your preferences, such as your language or font size, and to track your browsing activity across different websites.

Cookies can be classified into four main types:

- **Essential cookies:** Used to remember your login status, language preferences etc.
- **Performance cookies:** Used to collect information about how you use the website, such as the pages you visit and the links you click.
- **Targeting cookies:** Used to track your browsing activity across different websites.
- **Social media cookies:** Used by social media platforms to track your activity on their websites and to show you targeted advertising.

Cookies can pose a threat to your data privacy in a few ways. They can be used to track your browsing activity across different websites. This can be used for target marketing…or used by someone more sinister for spear-phishing.

To protect your data privacy, you can**…** Delete cookies regularly, block cookies, and use a privacy-focused browser.

Cookies aren't inherently good or bad… they're just part of the Internet. Thus it's important to protect the privacy of your online cookies.

For more information about managing internet cookies, call us at 248-362-3800 or visit: https://tinyurl.com/yfhfpu6b

Cybersecurity Skeletons In Your Business' Closet

Let's dive into a topic that might give you the chills—cybersecurity skeletons in the closet. You may not have old skeletons hidden away in the basement, but there's a good chance of cybersecurity vulnerabilities lurking in the shadows. Just waiting to wreak havoc.

You can't fix what you can't see. It's time to shine a light on these hidden dangers, so you can take action to protect your business from potential cyber threats.

Here are some of the most common cybersecurity issues faced by SMBs:

Outdated Software: The Cobweb-Covered Nightmare
Running outdated software is like inviting hackers to your virtual Halloween party.

When software vendors release updates, they often include crucial security patches. These patches fix vulnerabilities that hackers can exploit. Keep everything up to date to ensure that your digital fortress is secure.

Weak Passwords: The Skeleton Key for Cybercriminals
If your passwords are weak (or you reuse them over and over) you might as well be handing out your office keys to criminals.

Instead, create strong and unique passwords for all accounts and devices. Consider using a combination of upper and lowercase letters, numbers, and special characters.

Unsecured Wi-Fi: The Ghostly Gateway
Ensure your Wi-Fi is password protected. Make sure your router uses WPA2 or WPA3 encryption for an added layer of security. For critical business tasks consider a virtual private network (VPN). It can shield your data from prying eyes.

Lack of Employee Training: The Haunting Ignorance
Employee error is the cause of approximately 88% of all data breaches. Without proper cybersecurity training, your staff might unknowingly fall victim to phishing scams. Or inadvertently expose sensitive or personal information.

Regularly educate your team about cybersecurity best practices. Such as:
- Recognizing phishing emails
- Avoiding suspicious websites
- Using secure file-sharing methods

No Data Backups: The Cryptic Catastrophe
Imagine waking up to find your data is gone, vanished into the digital abyss. Without backups, this nightmare can become a reality.

Embrace the 3-2-1 rule. Have at least three copies of your data, stored on two different media types. With one copy stored securely offsite.

No Multi-Factor Authentication (MFA): The Ghoulish Gamble
Adding MFA provides an extra layer of protection. It requires users to provide extra authentication factors. Such as a one-time code or passkey. This makes it much harder for cyber attackers to breach your accounts.

Disregarding Mobile Security: The Haunted Phones
Ensure that all company-issued devices have passcodes or biometric locks enabled. Consider implementing mobile device management (MDM) solutions.

Incident Response Plan: The Horror Unleashed
Develop a comprehensive incident response plan. It should outline key items such as how your team will detect, respond to, and recover from security incidents. Regularly test and update the plan to ensure its effectiveness.

9 Reasons To Use Airplane Mode Even If You Are Not Traveling

Most people are familiar with their device's Airplane Mode.

You've probably used it when jetting off to exotic locations. But did you know that it's not just for globetrotters?

That's right! Airplane Mode isn't only for flying; it can be a handy feature for your everyday life.

Here are some top reasons why you should consider toggling it on, even if you're not traveling.

1. Save that precious battery life

2. Boost your charging speed (by about 4x)

3. A tranquil escape from Notifications

4. Focus Mode: Engaged!

5. Prevent embarrassing moments

6. Roaming woes, be gone!

7. A digital detox

8. Avoid unwanted radiation

9. Save data and money

"Congratulations on the discovery. Good luck getting it insured."

CartoonStock.com

Tips To Optimize A Dual-Monitor Setup

Two monitors are often better than one when it comes to getting things done efficiently.

A dual-monitor setup can significantly enhance your productivity. This is true whether you're a gamer, a creative professional, or just someone who happens to thrive on multitasking.

It's common for people to feel "off kilter" when trying to work from two monitors. The cause is usually the setup.

Here are some dual-monitor setup best practices to help you improve your two-screen experience and take it to the next level.

1. Match size and resolution

2. Get the right cables

3. Positioning is everything

4. Embrace the Extended Desktop

5. Focus on Taskbar Tweaks

6. Leverage Shortcuts

7. Mastering Multitasking