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 2025

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!"

How Lack of Preparation Can Affect Cybersecurity

Are you ready for a potential cybersecurity incident? From data breaches to insider threats, these digital risks lurk in wait for one misstep, so that hackers can break into your devices and network.

A lack of preparation in cybersecurity is like leaving your front door wide open in a storm. You're not just inviting trouble, you're practically rolling out the red carpet for it.

How does a lack of security preparedness play out in the digital world?

Consequences of Poor Cybersecurity Preparation

Without strong defenses, sensitive data like customer info, financial records, or intellectual property can be stolen or leaked.

Ultimately, our practice of daily cyber-hygiene protects us from easily-avoidable data breaches.

Simultaneously, unprepared organizations often scramble to respond to attacks, which has far-reaching consequences beyond the breach itself. This period of inactivity can lead to prolonged company outages and lost productivity. That all equals less money in the company budget, which directly affects your role at work. Those costs can even skyrocket due to ransom payments, legal fees, regulatory fines, and recovery expenses. In 2024, the cost of a data breach reached $4.88M on average.

If caused by a lapse of cybersecurity preparedness, some breaches might even violate certain data protection laws.

Continued on pg.2

Continued from pg.1

Failing to comply with data protection laws (like PCI, GDPR, Safeguards, or CCPA) can result in even more lawsuits and hefty fines.

Then, you also have to consider your customers or client base. Trust is hard to earn and easy to lose. A single breach can tarnish a brand's image for years, especially in industries like finance or healthcare. The damage to your reputation may be irreparable.

Why Preparation Matters

For small businesses, the blow from cyberattacks can be fatal. Around 60% of SMBs shut down within six months of a major cyberattack. Where would that leave you?

That's exactly why preparing for the worst ahead of time, makes your job easier during an emergency. Here's how you can proactively help your cyber-preparedness:

- Incident Response Plans: Without one, organizations face chaos during a breach. A well-prepared plan helps contain threats quickly and minimizes damage.
- Employee Training: Human error causes 95% of data breaches. Regular training helps you to recognize phishing attempts and follow best practices.
- Regular Updates and Backups: Outdated software and missing backups are open invitations for attackers. Preparation includes patching vulnerabilities and having recovery options ready.

In short, cybersecurity isn't just an IT issue — it's a business survival issue, and by extension, directly related to your job.

Conclusion

Preparation before a cyber-incident determines how much damage a data breach really does. In fact, practicing safe online behavior can prevent a majority of simplistic threats. Even if someone does sneak or hack their way into your company network, your proactive approach will mitigate much of the damage.

When organizations lack cybersecurity readiness, it's not just leadership that feels the impact. It affects every single team member too. We all play a part in keeping our systems safe, whether that means following security protocols, staying alert to threats, or participating in training. Preparation equals greater long-term cybersecurity.

Security Corner

Spoofing: When Trust Gets Faked

You hear warnings about phishing, ransomware, malware, but there's another threat that often flies under the radar: Spoofing.

What Is Spoofing?

There are two common spoofing tactics: Website spoofing and phone spoofing.

Website (URL) Spoofing: That feeling you get when a site looks almost like the one you trust; but tiny differences in the domain name, design, or URL raise your internal alarms.

Phone Number Spoofing (Caller ID Spoofing): You pick up the phone and the caller ID looks like it's coming from a friend, bank, police or a company you trust….but it isn't.

How to Stay Safe Against Spoofing

Here are some cyber-hygiene tips to help you stay safer every day:

- Always double check URLs before entering login information. Look at domain spelling (watch for swapped letters, extra words, etc.), use bookmarks for frequently accessed sites.
- Be skeptical of unsolicited calls or texts, even if the caller ID looks legitimate. If someone says they're from your bank (or your company, or tech support…), hang up and call back using a number you trust, not the one they gave you.

Spoofing can be convincing, and that's dangerous. Slow down and carefully assess any requests you get for private information, even if it "seems" legitimate.

For more information about this topic, call us at 248-362-3800 or visit: https://tinyurl.com/36c5x9ek

How To Use AI For Business Productivity While Staying Cyber-Secure

Most organizations have realized that AI is not a sentient system looking to take over the world, but rather an invaluable tool. They have come to utilize it to improve their productivity and overall operating efficiency.

AI solutions have been installed at an astounding rate. Some are used to automate repetitive tasks and to provide enriched data analysis on a previously unrealized level.

While this can boost productivity, it is also troubling from a data security, privacy, and cyber threat perspective.

The crux of this conundrum is how the power of AI can be harnessed to remain competitive while eliminating cybersecurity risks.

The Rise of AI

AI is no longer just a tool for massive enterprises. It is a tool every organization can use.

AI Adoption Risks

Organizations must understand that implementing any new technology needs to be done with thoughtful consideration of how it might expose them to various security threats.

• Data Leakage. In order to operate, AI models need data. This can be sensitive customer data, financial information, or proprietary work products. If this information needs to be sent to third-party AI models, there must be a clear understanding of how and when this information will be used.

• Shadow AI. Many employees use AI tools for their daily work. This might include generative platforms or online chatbots. Without proper vetting, these can cause compliance risks.

• Overreliance and Automation Bias. Many users consider AI-generated content to always be accurate when, in fact, it is not. Relying on this information without first checking it for accuracy can ultimately lead to poor decision-making.

Secure AI and Productivity

The steps necessary to secure potential security risks when utilizing AI tools are relatively straightforward.

- Establish an AI Usage Policy. It is critical to set limits and guidelines for AI use prior to installing any AI tools. Be sure to define approved AI tools and vendors, acceptable use cases, prohibited data types and data retention practices.
- Segment Sensitive Data Access. Adopting role-based access controls (RBAC) provides better restrictions on data access. It allows AI tools access to only specific types of information.
- Monitor AI Usage. It is essential to monitor AI usage across the organization to understand what and how information is being accessed and including which users are accessing which tools, what data is being sent or processed, and alerts for unusual or risky behavior. threats, deter email phishing, protect endpoints, and automate responses.
- Train Employees About Responsible Use. An unfortunate truth about humans is that they are the weakest link in the chain of cyber defense. Even the strongest defensive stance on cyber threats can be undone with a single click by a single user.

AI boosts productivity, but productivity without proper protection is a risk you can't afford. Contact us today for expert guidance, practical toolkits, and resources to help you harness AI safely and effectively.

Advanced Protection For Your Logins

Here are several advanced methods for securing your business logins:

1. Multi-Factor Authentication (MFA): MFA requires users to provide two verification points.

2. Passwordless Authentication: Some emerging frameworks have abandoned the username and password authentication method entirely.

3. Privileged Access Management (PAM): PAM solutions offer secure monitoring and the enforcement of 'just-in-time' access and credential vaulting.

4. Behavioral Analytics and Anomaly Detection: Modern authentication systems employ AI-driven methods to detect unusual behavior in login attempts.

5. Zero Trust Architecture: This architecture adopts the simple principle of "never trust, always verify."

How The Newest Black Friday Tech Gadgets Can Boost Your Business

Images of Black Friday no longer merely conjure up visions of bargain hunting shoppers bull-rushing storefronts to secure the best deals. It is now viewed by many organizations as a strategic opportunity to minimize the cost of upgrading their technology infrastructure.

Traditionally, Black Friday tech deals surrounded gaming platforms and entertainment technology, but that has changed. Now, businesses recognize that there are numerous deals on the latest technology that offer real-world value to improve collaboration and productivity.

"It's just a welcome mat. That doesn't count."

Best Practices When Buying Consumer Tech for Business Use

A quick look at online tech outlets shows just how steep the discounts can be on Black Friday. While these sales offer great savings, businesses need to approach purchases mindfully. Buying equipment solely because it's discounted defeats the purpose if it cannot integrate into your existing tech environment.

- Business-Grade Warranty: Unfortunately, consumer products don't offer the same commercial warranties or support. It is always a good idea to check this for any purchases organizations are considering.
- Secure Everything: Much like the warranty, not all consumer products come with the same safeguards necessary for enterprise-level security.
- Lifecycle Management: The discounted items need to be tracked and included in the IT management plan to determine when and how the devices will be replaced in the coming years.