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

February 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!"

What Should You Know About Incident Response?

Introduction

Good cyber resilience involves planning, testing and learning from incidents. How well do you know your company's incident response procedures? Do you have easy access to resources and reminders about where to report suspicious behaviors? Are there reminders around your workplace with I.T. support numbers and where to seek more information when there is an incident.

Organizations must assume breaches will occur and focus on rapid detection, containment and recovery. As a purveyor of sensitive data within the company, you are part of these procedures!

It's critical that you fully understand your role in the event of suspicious behavior or when faced with a full-on cyberattack.

What's Your Role?

Not only do you have a responsibility to the people whose private data you manage at work, but you also have to keep in mind that everyone and anyone can be a target of a cybercriminal.

Whether you work at a large organization or a very small business, cybercriminals target anyone they think is vulnerable! That's why it's important to have a plan in place, no matter how tech-savvy you are.

Here's the thing: you can't prevent every single cyberattack. In today's hyper-connected world, it's a matter of when—not if. 95% of cyberattacks begin because of

Continued on pg.2

Continued from pg.1

simple, human error. Therefore, it's of paramount importance that you have procedures in place that explain what to do when you spot abnormal system behavior and where to go in order to report malicious encounters.

The Impact of Cyber Resilience

There's good news amidst the danger! With a proper incident response plan in place, you can be prepared to bounce back quickly. In an emergency situation, you don't want to waste time panicking about where or how to send up red flags. You want to jump right into damage control, thereby minimizing the negative fallout of a breach.

That's where cyber resilience comes in. Think of it like your digital fire drill. By planning, testing, and learning from any hiccups, you'll be better equipped to handle whatever comes your way.

So, what can you do?

- Plan ahead. Take some time to think about the things you absolutely can't afford to lose. Is it precious family photos? Important work documents? Once you know your priorities, you can figure out how to back them up securely (think external hard drive or cloud storage).
- Be ready with automatic detection software. Antivirus software is a must-have. Most programs will also monitor for suspicious activity and alert you if something seems off.
- Practice makes perfect. Just like a fire drill, put your plan into action! Test your storage systems and backups, to guarantee they work well before an incident occurs. This way, you won't be scrambling in a crisis.
- Learn from every incident. Even minor hiccups can be valuable lessons. If you do get hit by a cyberattack (like malware or phishing), take some time to figure out what happened and how you can prevent it from happening again.

Conclusion

Incident response is no joke. When a serious security incident hits you or your company, there are really important steps that need to be taken AS SOON AS POSSIBLE to minimize the repercussions of that event.

Remember: Cybersecurity isn't about being perfect, it's about being prepared. By taking some simple steps, you can make your digital life a whole lot more secure!

Security Corner

Why Is Email Such A Common Method Of A Cyber-Attack?

Did you know that 94% of all malware is delivered via email?

Why is that? Let's find out together!

Why Do Cybercriminals Prefer Email?
Email is ubiquitous – almost everyone uses email for personal and professional communication. With billions of email accounts worldwide, attackers have countless opportunities to reach potential victims.

Weaknesses in Email Platforms
Modern email-based malware attacks are becoming increasingly sophisticated, and can exploit common technical risk factors, such as…

- Difficulty in comprehensively scanning all attachments and links.
- Legacy email systems with outdated security measures. Traditional security filters that can't handle multi-stage attacks.

The Allure of Social Engineering
Many successful attacks exploit human behavior, such as curiosity or urgency. *Phishing emails* often use social engineering tactics to trick recipients into clicking on malicious links or downloading infected attachments.

Emails are particularly effective for social engineering attacks. Cybercriminals can craft convincing messages that:

- Appear to come from trusted sources like banks, colleagues, or familiar organizations.
- Manipulate recipients into taking quick, thoughtless actions like clicking a link or downloading an attachment.

For more information about email-based cyber attacks, call us at 248-362-3800 or visit: https://tinyurl.com/mtknsazy

What Is Blockchain Technology And How Does It Work?

Blockchain technology is changing the world. It is a system designed to keep records safe and secure. But how does it actually work?

What is Blockchain?
Blockchain is some kind of digital ledger. In it, information is stored in a manner that makes it hard to change. This ledger is shared among many computers, each one having a copy of the same ledger.

Information is kept within blocks. Each block maintains a list of transactions. As the block gets filled, it connects to the previous block, forming a linked chain of blocks or a blockchain.

How Does Blockchain Work?
Blockchain works by mining. Miners are computers that solve complex math problems. Once they solve these problems, they add new blocks to the chain and the process repeats.

Each block has a unique code called a hash. This hash helps keep the information secure. If anyone tries to change the information, the hash also changes. That way, it makes it very easy to spot any tampering.

Why is Blockchain Secure?
The blockchain is secure because it is made using cryptography. Cryptography is like a secret code used to protect information. Only the ones who have the right key will be able to read it. Besides, blockchain is decentralized. That means no one controls it. Several computers are working together to keep it safe.

What Are the Uses of Blockchain?
Many other uses of blockchain exist beyond money. It can track goods in a supply chain, store medical records safely, and help with voting in elections.

In finance, blockchain powers cryptocurrencies such as Bitcoin. These are online digital currencies.

How Does Blockchain Impact Our Lives?
Blockchain makes transactions faster and cheaper. It removes the need for middlemen like banks. This saves time and money.

It also introduces transparency. Users can view all the transactions made on the blockchain. These actions help to establish trust among users.

What Are the Challenges of Blockchain?
There are challenges regarding the use of blockchain. Much of the mining is power-consuming. This might not be suitable for the environment.

Besides these issues, there are even more regulatory ones. Governments and agencies don't yet know how to deal with blockchain technology.

What's Ahead for Blockchain?
The future of blockchain is very bright. More and more industries are exploring its potential every day. In healthcare, it can secure patient data and streamline access to patient records.

In entertainment, it can protect intellectual property and ensure fair compensation for creators.

Financial services are also benefiting from blockchain, with faster and more secure transactions. Developers are working on making blockchain more efficient and eco-friendly, addressing environmental concerns.

Blockchain technology is fascinating and holds immense potential. It can transform various aspects of our lives for the better. For example, it enhances security by safely storing and sharing data, which is crucial in healthcare. Its transparency and immutability foster trust, making it ideal for supply chain management. Its decentralized nature makes systems more resilient, while smart contracts automate transactions, increasing efficiency.

5 Common Cyber Threats In 2025

- Phishing attacks will always be in vogue. They make you give away your personal data. Always check the sender's email address. Do not click on suspicious links.
- Ransomware locks your files and demands money to unlock them. Keep your software updated and back up your files regularly.
- Malware is bad software that may cause damage to your computer. Use antivirus software and avoid downloading files from unknown sources.
- Cybercriminals will leverage artificial intelligence for more sophisticated attacks. AI supports them in selecting the right victims.
- There are more and more devices connecting via the internet. Make sure that all devices have updated security measures on them.

Best Practices For Secure Data Backup

Data backup refers to the creation of a copy of your data. The copy can be used in the event of loss or destruction of the original data.

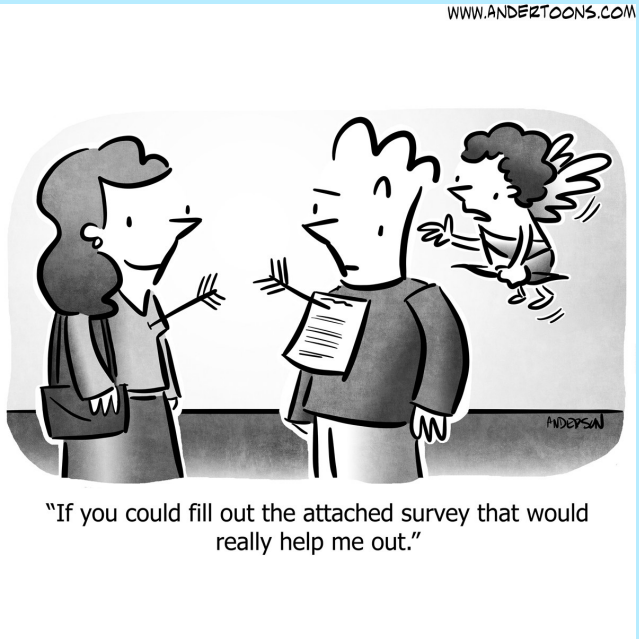
Backups can be stored on various devices, such as external hard drives, or in the cloud. Having a backup ensures you don't lose important information.

Here are best practices for secure data backup:

• **Use Encryption**: Encryption scrambles your data so only you can read it. This keeps it safe from hackers.

• **Set Strong Passwords**: Use strong passwords for all your backup accounts and devices. This prevents unauthorized access.

• **Regularly Test Your Backups**: Testing ensures that your backups work properly. Try restoring a file to make sure everything is correct.



"If you could fill out the attached survey that would really help me out."

9 AI Tools You Need In Your Office For Productivity

- **Smart calendars** use AI to manage your schedule.

• **Task managers** put your tasks in order by deadline or urgency.

• **Email assistants** can filter important emails and even draft replies for you.

• **Virtual meeting helpers** use AI to transcribe meetings in real time.

• **Data visualization** tools create simple charts and graphs that are easy to understand.

• **Predictive analytics** make use of AI to forecast the future with the help of data related to the past.

• **Writing assistants** can help with grammar checks and content ideas.

• **Design tools** powered with AI will create stunning visuals in a jiffy.

• **Chat bots** are AI programs that chat with customers online.