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

January 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!"

Cyber Extortion Is NOT Just A Concern For Your Boss

Introduction
Cyber extortion…it's exactly what it sounds like. This form of cybercrime occurs when attackers gain unauthorized access to a company's sensitive data or systems and then demand a ransom to stop the attack or return control to the victim.

Common types of cyber extortion include ransomware, distributed denial-of-service (DDoS) attacks, and brute-force data extortion. These are all digital methods for attackers to pry money and sensitive information from the organization under duress!

What That Means For You
Now, you may be thinking…what does that have to do with you?! As an employee, understanding cyber extortion is important because it can directly impact your work environment and responsibilities. Here are a few ways it might relate to you!

- Data Security: If your company falls victim to a cyber extortion attack, sensitive data, including personal information of employees and customers, could be compromised.
- Operational Disruption: Cyber extortion can disrupt business operations, leading to downtime and affecting your ability to perform your job.
- Financial Impact: The costs associated with cyber extortion, including ransom payments and recovery efforts, can affect the company's financial health, potentially impacting budgets and resources.
- Reputation Management: If a cyber extortion incident becomes public, it can damage the company's reputation,

Continued on pg.2

Continued from pg.1

which might affect employee morale and customer trust.

By staying informed and vigilant, you can contribute to your company's cybersecurity efforts and help mitigate the risks which are associated with cyber extortion.

How Businesses Are Negatively Impacted
Cyber extortion can have significant ramifications for a company, impacting various aspects of its operations and overall health. Let's begin with the biggest concern: Finances. Companies may face substantial financial losses due to ransom payments, recovery costs, and potential fines for data breaches. For instance, many organizations end up paying the ransom in ransomware, which can exceed $100,000 (not to mention it won't guarantee that you get your data back, or that the hacker won't leak confidential information on the Dark Web anyway).

The downtime caused by disrupted business operations typically also results in lost productivity, which can affect the company's ability to serve customers and meet business goals!

There are also regulatory and legal considerations when a cyber extortion event occurs. Companies may face legal actions and regulatory fines if they fail to protect sensitive data, thus compliance with cybersecurity regulations becomes even more critical to avoid these penalties.

Conclusion
Understanding these potential impacts can help companies better prepare and respond to cyber extortion threats. Meanwhile, the stress and uncertainty caused by such an incident can affect employee morale and productivity, hence you should reach out to your superiors now if you have any questions about communicating your concerns and any suspicious activity! Having support when your company is experiencing a cyber extortion attack can help you stay calm and protect as much of your private data as possible.

Just remember, cyber extortion doesn't only happen at work — and it can have just as big of an impact on your personal data and systems. If a hacker tries to pressure or force you into divulging private information or even sending them money, take a breath to remind yourself that you should never pay a cyber extortion fee. Most likely, the hacker will still run off with your money AND your private files, too.

By understanding what threats you (and your organization) face, and how you can protect against such cyber extortion attacks, you can more effectively safeguard all of the private information under your care — and keep your data secure, too!

Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

IT BUYERS GUIDE
What Every Business Owner MUST Know About IT Support Services And Fees
What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.
- **Claim your FREE copy today at https://www.cti-mi.com/itbuyersguide-125/**

Security Corner

How to Outsmart Insider Threats

Insider threats are evolving in sophisticated ways, and they continue to pose significant risks to our workspaces today. Whether it's a coworker forgetting to lock the drawer housing the most important contracts, a third-party vendor unknowingly bringing malware into the company network, or a threat actor posing as your I.T. guy to directly steal company secrets, insider threats are extremely dangerous to your personal data!

3 Biggest Insider Threats to Watch Out For Today

1. Data Exfiltration with AI Tools- The rise of AI-based tools has made it easier for employees to capture and transfer sensitive data. Watch out for unauthorized usage of such tools in sensitive contexts.
2. Financial Fraud and Social Engineering- Financially motivated employees could manipulate transactions, use credentials of former employees, or engage in insider trading with proprietary information.
3. Data Deletion or Corruption by Disgruntled Employees- Employees with access to databases or files might be tempted to delete or corrupt data as an act of retaliation, especially if they feel underappreciated or are about to leave the company.

By staying proactive and fostering a culture of security, you can help mitigate these insider threats in your workplace. As the new year dawns, let's pledge to keep up to date on our security awareness trainings, report suspicious behavior when we see it, and learn the avenues for responding to threats from anyone inside OR outside of the organization.

For more information about insider threats, call us at 248-362-3800 or visit: https://tinyurl.com/4x2taxyu

What Is Threat Exposure Management (TEM) And Why You Need It?

Threat Exposure Management (TEM) is an important cybersecurity tool. It helps organizations find and fix weak spots in their systems. TEM outsmarts hackers before they get into your network.

How TEM Works
TEM uses special software to scan your entire network. It finds places hackers could attack and helps you fix these weak spots.

Continuous Monitoring
TEM keeps looking all the time. This way, you can find new problems as soon as they appear.

Risk Assessment
TEM finds which weak spots are the most dangerous. This helps you fix the most important ones first.

Main Parts of a TEM Program

Asset Discovery
This finds all devices and software on your network. You can't protect what you don't know about!

Vulnerability Scanning
This looks for open weak spots in your system. It's like checking for unlocked doors in your house.

Threat Intelligence
This provides insights into new hacker techniques, helping you to know to watch out for.

Remediation Planning
Once you find the vulnerabilities, you need a plan to fix them. TEM helps you determine how to patch these spots.

Benefits of TEM for Your Business

Better Security
Fixing weak spots makes your whole system much safer and more resilient.

Cost Savings
Stopping an attack before it happens can save you a lot of money. Dealing with the aftermaths of cyber attacks often comes with expensive costs.

Peace of Mind
With TEM, continuous monitoring ensures your system is always under watch. This can help you worry less about cyber attacks.

What to Look for in a TEM Solution
A good TEM tool should:

- **Be user-friendly**, ensuring that all team members, regardless of their technical expertise, can easily navigate and utilize the tool.
- **Provide immediate results**, enabling quick and effective decision-making to address potential threats as soon as they are detected.
- **Integrate seamlessly** with your existing security infrastructure, enhancing overall protection by working in harmony with other security tools and systems.
- **Generate clear and comprehensible reports**, presenting findings in an easily digestible format that facilitates understanding and corresponding action by all stakeholders.

Getting Started with TEM

- **Check your current security setup** to understand your existing vulnerabilities and areas for improvement.
- **Find a TEM tool that fits your needs**, ensuring it aligns with your security goals and integrates well with your current systems.
- **Set up the tool** and start scanning your environment.
- **Make a plan to fix the weak spots you find**, prioritizing and addressing the most critical issues.
- **Keep scanning** and improve your security continuously, regularly updating your strategies and tools to stay ahead of emerging threats.

How Password Managers Protect Your Account

A password manager keeps all your passwords in one place. Think of it as a digital safe for your login information.

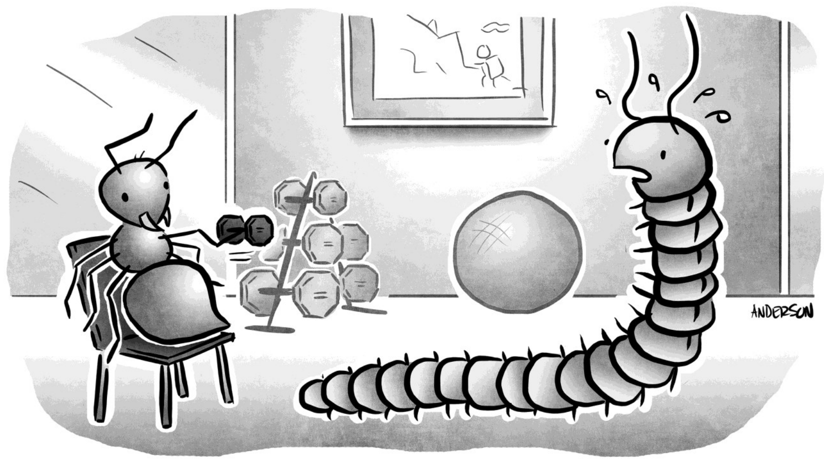
You only need to remember one password, the master password. This master password lets you access all your other passwords.

Why Use a Password Manager?

- **It Helps You Create Strong Passwords**. Password managers generate long, random passwords that are hard to crack.
- **It Remembers Your Passwords**. With a password manager, you don't need to memorize many passwords. The tool does this for you.
- **It Keeps Your Passwords Safe.** Password managers use high-level security to protect your data. Even if someone hacks the password manager company, they can't read your information.

Features of Password Managers

- **Password Generation**: Good password managers can create unique passwords for you.
- **Auto-Fill**: Many password managers can fill in your login information on websites. This saves time and avoids typos.
- **Secure Notes**: Some password managers let you store credit card numbers or important documents.
- **Password Sharing**: Some tools let you share passwords safely with family or coworkers.



"Man I hate leg day."

How to Choose a Password Manager

- Find one with strong encryption and two-factor authentication.
- The manager should be easy for you to understand and use.
- Research the features you want and the price you can afford.

Do You Really Need Dark Web Monitoring?

Dark web monitoring looks for your information on the dark web. It can find stolen passwords or credit card numbers. This helps you know if someone stole your data.

But is dark web monitoring really necessary? Here are the most important benefits to consider:

- **Identity and business protection**. It helps you know if someone stole your personal or business data. You can then change passwords and further protect yourself.
- **Real-time alerts when your information is stolen**. The tools alert you right away when they find your information on the dark web
- **Protection for passwords, credit card numbers, social security numbers, and more**. This enables you take quick, specific actions.