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

July 2024

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 Are Supply Chain Attacks Targeting Critical Infrastructure?

Introduction

Supply chain attacks are not new cyber-threats. For a long time now, cybercriminals have gone after the services that *our* services rely on instead of spending time targeting each individual. Ultimately, the goal is the same: to steal as much of *your* personally identifiable information (PII) as is possible.

Cybercriminals are increasingly targeting the supply chains of critical infrastructure providers, such as power grids and water treatment plants. These attacks can have a devastating impact on society and are likely to become *even more common* in the coming years.

Why Critical Infrastructure?

First, let's define "critical infrastructure" in case you aren't aware. It refers to the backbone systems that keep our society functioning, like power grids, water treatment plants, transportation networks, and healthcare facilities.

In other words, it's the systems that society can't effectively function without! We all rely on critical infrastructure to make our day-to-day lives more convenient and take advantage of twenty-first century technology.

Critical infrastructure systems often hold sensitive data about individuals, including PII (Personally Identifiable Information). By attacking the supply chain, attackers gain access to this data for various malicious purposes, such as identity theft, fraud, and blackmail.

Unfortunately for us, threat actors have increasingly targeted these systems in recent years. Supply chain attacks, whose risks and uncertainties often interrupt the

Continued on pg.2

Continued from pg.1

operational efficiency of the supply chain, often have adverse impacts on an organization *as well as* everyone in it. Cybercriminals don't have to target *your* Facebook profile if they can take over Facebook itself, or sneak in via the third-party that Facebook hires to take customer complaint calls.

By compromising a single vendor used by many critical infrastructure providers, attackers can gain access to multiple targets with minimal effort. Threat actors also tend to target the weakest link, because smaller supply chain partners often have less robust cybersecurity measures due to limited resources and expertise. Attackers exploit these vulnerabilities to gain a foothold and then pivot to the more protected critical infrastructure systems.

How does this all come back to you? Businesses tend to trust their established vendors, relying on their security practices and knowing that they have always been secure in the past. This trust creates a blind spot for attackers to exploit, infiltrating seemingly safe systems through compromised products or services. You don't have to fall for their tricks at all, and they could still get your PII.

Conclusion

If a cyberattack successfully breaches critical infrastructure through a supply chain vulnerability, the perpetrators could steal large amounts of PII, including names, addresses, Social Security numbers, financial information and medical records. This exposes individuals to the risk of identity theft, financial loss, and medical privacy violations.

On a larger scale, compromised critical infrastructure can lead to disruptions in essential services like electricity, water, communication and healthcare. This can significantly compromise our health and safety!

When critical infrastructure is compromised, it erodes public trust in these systems and the organizations responsible for their security. To protect your PII from supply chain cyberattacks, it's up to YOU to take proactive measures!

- **Be cautious about sharing personal information online and with unknown entities.**
- **Use strong passwords and enable two-factor authentication.**
- **Stay informed about cyber threats and scams.**
- **Report any suspicious activity to the relevant authorities.**

By taking these steps, we can collectively build a more secure and resilient cyber environment that protects our critical infrastructure and safeguards our PII!

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

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-724/

Security Corner

Don't Blur The Lines Between Work And Personal Devices!

We've all been there. A quick scroll through social media during a lull in the workday or checking a personal email on your work phone. In today's fast-paced world, convenience often reigns supreme. Although it may be convenient sometimes, unfortunately when it comes to our devices, blurring the lines between work and personal can pose significant cybersecurity risks!

An Overview of Keeping Things Separate

Let's face it, there's an undeniable appeal to using one device for everything. It's readily available, eliminates the need to constantly switch back and forth, and for some, separate work and personal devices might not be an option.

However, this convenience comes at a high cost

- **Security weaknesses**. Personal browsing or downloads can introduce malware or viruses that could then infect the work network.
- **Data exposure.** Work devices often contain sensitive information. If your personal browsing habits get you to a phishing site, for instance, your work data could be exposed.
- **IT monitoring**. Many companies' IT teams monitor work device activity, so your personal browsing could be seen by your employer.
- **Privacy concerns**. Even if your employer isn't monitoring, you might not want them to have access to your personal information.

Bottom line is that mixing your work and personal devices can have consequences at work, lead to data privacy concerns and security breaches,

For more information about managing personal and work devices, call us at 248-362-3800 or visit: https://tinyurl.com/4377dyyx

Is Your Business Losing Money Because Your Employees Can't Use Tech?

Shiny new tech can be exciting! It promises increased efficiency, happier employees, and a competitive edge. But that promise can turn into a financial nightmare if you neglect employee training and change management.

When employees have trouble using their business tools, productivity drops. Mistakes can be made, and customer service can fall.

Lack of Technology Training

Imagine investing in a top-of-the line CRM system. Then you see your sales team floundering instead of excelling. They can't find key features, struggle with data entry, and miss deadlines.

Why? Because they haven't been properly trained on the new software. It leads to the following costs: including loss of productivity, costly errors and demotivation and resistance.

Failing to Manage the Change

New technology disrupts workflows. Without proper change management, employees feel overwhelmed.

The goal is to help them transition successfully with proper training and support. When companies neglect change management, the following can happen:

- Low Morale
- Use of Shadow IT
- Resistance to Future Improvements

Building a Bridge to Success

So, what is the key to unlocking the true value of new technology? It lies in effective training and implementing change management.

Here's how to avoid the negative costs and get the full benefits from your tech.

- ***Invest in Comprehensive Training –*** Don't treat training as an afterthought. Yes, some tools say they're easy to use. But people have different tech literacy levels. Develop a tailored training program that goes beyond basic features. Include video tutorials, hands-on workshops, and ongoing and easy to access support resources.
- ***Focus on User Adoption, Not Just Features –*** Training shouldn't just explain how the software works. It should focus on how the new system will benefit employees in their daily tasks and improve workflow efficiency. If employees don't adopt the new solution, the project fails.
- ***Embrace Change Management –*** Communicate the "why" behind the change. Explain how the new technology will make everyone's jobs easier. Encourage open communication and quickly address concerns.

The Takeaway

New technology is a powerful tool, but it's only as valuable as its users. Prioritize employee training and change management. This will help you bridge the gap between a shiny new system and a real return on investment.

Happy, well-trained employees using the right tools are your secret weapon. They can help you maximize efficiency, boost morale, and stay miles ahead of the competition

7 Easy Steps To Building A Culture Of Cyber Awareness

Cyberattacks are a constant threat in today's digital world. Phishing emails, malware downloads, and data breaches. They can cripple businesses and devastate personal lives.

Building a cyber awareness culture doesn't require complex strategies or expensive training programs.

Here are some simple steps you can take to make a big and lasting difference.

1. Start with leadership buy-in
2. Make security awareness fun, not fearful
3. Speak their language
4. Keep it short and sweet
5. Conduct phishing drills
6. Make reporting easy and encouraged
7. Security champions: empower your employees

Smart Tips For Building A Smart Home On A Budget

Imagine a world where your lights turn on automatically as you walk in the door. Your coffee starts brewing before you even crawl out of bed. A simple voice command adjusts the temperature to your perfect setting.

This is no longer just something out of a sci-fi movie. Today's smart technology seamlessly integrates with your daily life. It can create a more convenient, comfortable, and even secure living space.

Here are some tips to transform your humble abode into a tech-savvy haven affordably:

1. Start small and scale up
2. Think beyond the big brands
3. Repurpose what you already have
4. Leverage free smartphone apps

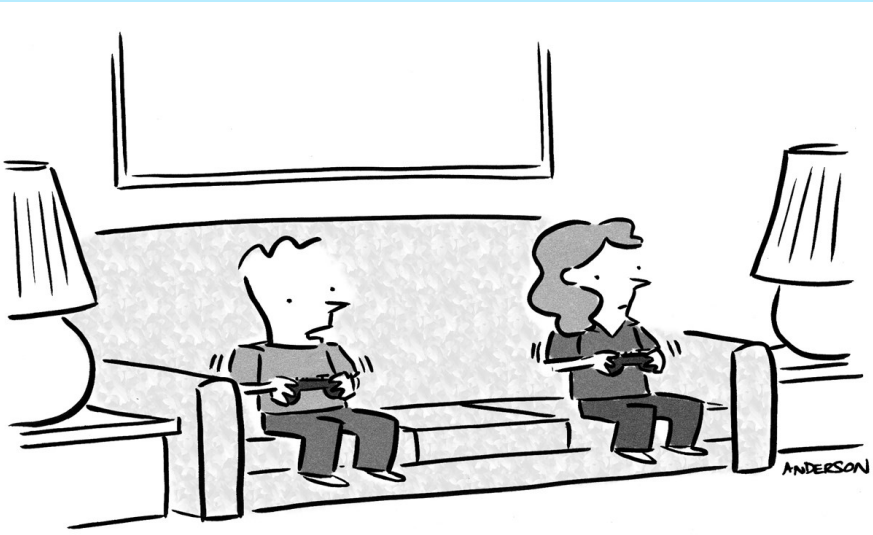
Why Continuous Monitoring Is A Cybersecurity Must

Cyber threats are constantly evolving, and traditional security measures are no longer enough. Continuous monitoring acts as your vigilant digital guard. It's constantly checking for weaknesses. It sounds the alarm before attackers are able to exploit them.

Here's why continuous monitoring is a cybersecurity must:

- Breaches Happen Fast
- Advanced Threats Need Advanced Defenses
- Compliance Requirements Often Mandate It
- Peace of Mind and Reduced Costs
- Faster Incident Response
- Compliance Reporting

In today's threat landscape, continuous monitoring is not a luxury. It's a security necessity. Don't wait for a security breach to be your wake-up call.



"It's interesting - Mom hates early Christmas sales, but she *loves* early back-to-school sales."