Connection

December 2024

We believe that experienced, reputable, and fast responding IT support should be the standard!

There are 3 Grinches in this newsletter—see if you can find all 3 before he steals Christmas!

Our Services:

- Data Backup & Recovery
- Managed Services
- IT Consulting
- Network Security
- Cloud Computing
- Remote IT Services
- Cyber Security Training
- Mobile Device Management
- VoIP Phones

Let's get social!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

LinkedIn:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Digital Newsletter:
www.csuinc.com/news

Are You Managing Your Vendor Security Risks?

As the year comes to a close, businesses often take stock of their successes and identify areas for improvement. While finalizing projects and setting goals for the upcoming year are top priorities, there's one crucial task that shouldn't be overlooked: managing vendor security risks. Vendors are essential to your operations, but they can also pose a significant cybersecurity threat if not properly vetted and monitored—especially when handling sensitive data

What is Vendor Risk?

Many companies depend on third-party vendors, like cloud service providers or file-sharing platforms, to run day-to-day operations. But when one of these vendors falls victim to a cyberattack, your sensitive data is at risk. A recent example is the 2023 MOVEit Transfer breach, where attackers exploited software vulnerabilities, gaining access to critical business data, including customer records, for thousands of

(continued on page 2)

organizations. According to BlueVoyant's State of Supply Chain Defense report, businesses experienced an average of 4.16 supply chain breaches in 2023, disrupting operations and causing significant damage.

Vendor-related breaches aren't just a headache—they can lead to data loss, customer trust issues, and even legal complications. As you wrap up this year, consider incorporating these best practices into your vendor risk management strategy:

1. Review Vendor Contracts

Your vendors need to be held accountable for maintaining strong security practices, such as encryption, secure data storage, and incident response. Start by reviewing your existing vendor contracts to ensure they include key security clauses. Make sure expectations are clearly outlined so that both you and your vendors understand your security responsibilities.

2. Conduct Vendor Security Audits

If you haven't done so recently, now is the time for a thorough security audit of your high-risk vendors. This will help you assess whether they are implementing critical cybersecurity measures—like multifactor authentication, encryption, and regular system updates. Understanding your vendors' security posture helps you better protect your own systems.

3. Monitor for Emerging Risks

Cyber threats are constantly evolving, and so are the risks your vendors face. Regularly monitor your vendors' security practices, track any vulnerabilities or breaches, and stay up-to-date on emerging threats. This proactive approach will help you identify and address potential risks before they escalate.

4. Update Your Vendor List

Now is a great time to "clean house." Consider terminating relationships with vendors who aren't meeting your security standards, and strengthen ties with those who are proactive about safeguarding your data. It's also a good idea to establish clear onboarding and offboarding procedures for vendors, ensuring that former vendors no longer have access to your systems or data.

5. Refer Us to Your Vendors!

If your vendors need IT support to secure both their data and yours, send them our way! Through our referral program, you could even earn some extra cash. Why not take advantage of this opportunity?

By implementing these, you can ensure that your vendor relationships contribute to your overall cybersecurity strategy, rather than exposing you to security risk.

Tech Giggles!

Why did the computer keep freezing?

...

It had too many windows open!

Tech Gifts to Avoid

While a fun robot that uses facial recognition to read your nephew's moods might sound like an amazing gift, it's important to consider the security risks involved. Devices like this can be vulnerable to being hacked or used for third-party advertising. At the 2023 CES electronics exhibition, Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, pointed out that many tech companies tend to focus on cost and speed rather than safety.

Here are some tech gifts you might want to avoid, along with some tips for smarter shopping:

Camera-Enabled Devices with Weak Privacy Policies:

Devices like doorbell cameras are designed to capture everything happening around your home. If they're not well-secured, hackers could access live feeds and track when you're away. Always choose cameras that offer end-to-end encryption and have clear privacy policies.

AI-Integrated Devices:

In 2022, images from iRobot's AI-enabled Roomba were leaked online, raising questions about data privacy. Always check the privacy policy to see how your data will be used. If you can't customize your settings or if the company isn't clear about their practices, it might be best to skip it.

Tracking Devices for Kids:

Tracking devices for kids can seem like a thoughtful gift, but they might expose your child's location to unwanted eyes. For example, the app Life360 was found to be sharing user location data with third parties. A better approach is to have open conversations with your kids about location sharing and consider built-in options like Google's Family Link or Apple's encrypted location sharing.

Genetic Testing Kits:

In 2023, a significant number of 23andMe users had their data hacked, which is a reminder of the risks involved in genetic testing. Sensitive information can attract unwanted attention, and companies have faced data breaches. Plus, law enforcement may access this information. Keep in mind that once you provide your DNA, you're sharing your genetic data—and that of your relatives too.

When shopping for tech gifts, keep these risks in mind to make choices that keep everyone safe and happy!

Holiday Travel Awareness

As holiday travel picks up, hackers see a prime opportunity to exploit travelers who may let their guard down on their digital security. Security risks like phishing, public Wifi and lost devices can easily compromise your personal information during travel. But its not just your data at stake – when employees let their guard down, they can unknowingly open the door to threats for their entire company.

According to World Travel Protection, only about 30% of companies require employees to follow basic cyber security measures while traveling. This leaves a significant gap in protection, potentially exposing entire organizations to serious risk. Here's how to safeguard yourself and your business during busy holiday travel.

Safety Tips Before & After a Trip:

To avoid the stress of lost devices, stolen data or a security breach that could ruin your trip, make cyber security a priority by taking a few simple steps before during and after your journey:

Before traveling:

1. Update all devices
Software updates often include patches for security vulnerabilities

2. Backup important data
If your laptop containing vital client presentations is stolen, a cloud based or other security backup will allow you to get your data back without significant disruption.

3. Use Multifactor Authentication
MFA adds an extra layer of security by requiring more than just a password to access accounts. This makes it much harder for hackers to gain access, even if they have your password.

4. Restrict Access to Sensitive Data
If you don't need certain files or applications while on the road, temporarily remove access. This reduces the risk of compromised sensitive information if your device is stolen or hacked.

5. Secure your Device
Ensure all devices are password protected and encrypted. Encryption scrambles your data, making it unreadable to unauthorized users.

While Traveling:

1. Avoid public Wifi
If you must connect, use a virtual private network (VPN) to encrypt your Internet traffic. This acts as a secure tunnel between your device and the internet, protecting your data from prying eyes.

2. Be cautious of Public Charging Stations
Public USB charging stations can be compromised by attackers looking to steal data or install malware on your device – a practice known as "juice jacking." Plug your charger into an electrical outlet or use a USB data blocker, which can prevent data transfer.

3. Never leave Devices Unattended
Always keep your devices with you or securely locked away. If you must leave your laptop in your hotel room, use a physical lock to store it. Never

hand your device to strangers, even if they appear to be offering help.

4. Disable Bluetooth

Turn off Bluetooth when not using it, especially in public places. Hackers can exploit open Bluetooth connections to gain access to your device

5. Pay Attention to Online Activity

Phishing, business email compromise and online shopping scams are common during the holiday season. Always verify the authenticity of emails, especially those requesting sensitive information or urgent action.

Returning Home:

Security awareness doesn't stop once you get home. Sometimes, you dont know until you return that you've been hacked.

1. Review Account Activity

Once you're back home, review your accounts and look for unusual logins or transactions you didn't initiate.

2. Change Passwords

If you accessed sensitive information while traveling, it's a good idea to change your passwords when you get home. This ensures that any potential compromises during your trip don't lead to long-term issues.

Consider a Travel Policy:

To further protect your business, consider implementing a company-wide travel cyber security policy. This policy should outline the expectations and procedures for employees traveling on business or working remotely. Key elements to include are:

Guidelines for using public networks
Reporting lost or stolen devices
Responding to potential security incidents

Following these simple steps will significantly reduce travel-related cyber security risks and ensure that you can travel with peace of mind.

8 STRATEGIES FOR TACKLING "TECHNICAL DEBT" AT YOUR COMPANY

Think of technical debt as the interest you pay on a loan you never intended to take. As your system grows, those hasty decisions can cost you in the long run.

Here's how to address it:

- *Identify and Prioritize.* Focus on the most critical issues that will drive the most value first.
- *Integrate Debt Management into Your Workflow.* Maintain a balance between new development and debt reduction.
- *Educate and Train Your Team.* Foster a culture of quality thinking.
- *Improve Documentation.* It provides a reference for current and future team members.
- *Regularly Update and Refactor Systems.* This involves making small, manageable changes for quality.
- *Optimize Security Practices.* Helps maintain system reliability and performance.
- *Manage Dependencies.* Tracking ensures compatibility and security.
- *Foster a Culture of Continuous Improvement.* Encourage learning, celebrating successes, and regular reflection to drive ongoing enhancement

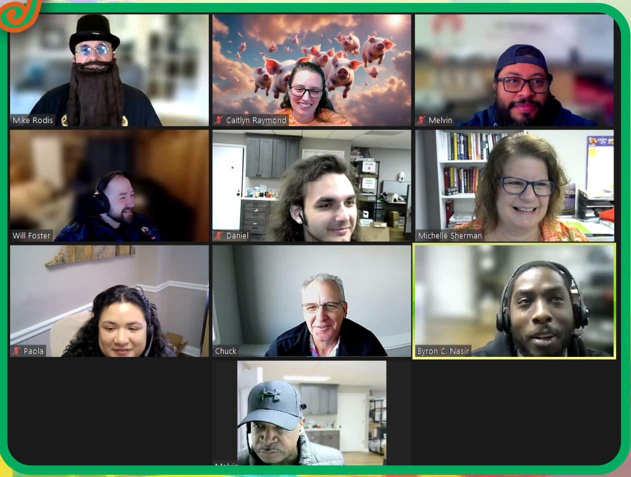
What's NEW at CSU?

Family PJ Day!

Whats the most comfortable day? PJ Day! While the work from home-rs had no change, we office folk loved the cozy work attire!

Absurdity Day

Absurdity day was a blast! Chair exchanges, a zoom visit from a long lost employee, team faces hidden around the office, and other fun absurd things occured! You can see more on our Facebook page!



A Holiday Tech Poem for You

By: Faye the Elf

‘Twas the season of tech, and all through the net,
Not a virus was stirring, not a bug to beget.
The servers were humming, the networks secure,
Thanks to Computer Services, peace is ensured!

Our techs work with care, to solve all your woes,
With firewalls, encryption, and solutions that glow.
We guard your devices, protect every byte,
So you can relax, and sleep sound through the night.

If you know someone in need of our aid,
A referral would make our Christmas parade!
No greater gift could you give, it’s true—
A trusted friend helped by us, just for you.

So here’s to safe browsing, and problem-free days,
From our IT family, we send holiday praise!
Merry Christmas to you, and a Happy New Year,
From Computer Services—your network’s safe here!

Hockey fights cancer night with the CSU team! What a fun night! Although the Caps lost, it was great to take time to celebrate cancer survivors and those going through treatment.