

TECH BTYES

October 2024

Stay updated with our monthly tech and cybersecurity insights. Get the latest innovations, tips, and stay secure!



Keep up with the newest advancements and trends in technology.

Matthew DeWees

-President

Think of employee cybersecurity training as an ongoing process, not a one-time event. Hackers constantly evolve their tactics, so your training must keep pace. Regular evaluations help identify strengths and weaknesses.

Your team might excel at spotting phishing emails but still fall for strong password scams. By continuously updating your training, you're not just educating your employees; you're creating a human firewall capable of adapting to any cyber threat.

Need help with cyber awareness training? Contact us at everythingit@virtualdataworks.com to schedule a chat.

Until then, stay safe,



President - Virtual DataWorks

WHAT'S INSIDE?


- 02** WHY SECURING YOUR SOFTWARE SUPPLY CHAIN IS CRITICAL
- 03** TACKLING "TECHNICAL DEBT" AT YOUR COMPANY
- 04** MOBILE-OPTIMIZED WORKSPACE
- 05** COMMON MOBILE MALWARE TRAPS
- 06** TROUBLESHOOT COMMON BUSINESS NETWORK ISSUES
- 07** WHAT IS A PASSWORD MANAGER AND WHY IS IT USEFUL?


DID YOU KNOW?

The first domain name ever registered was **Symbolics.com**? It was registered on March 15, 1985, and it's still online today!

Virtual DataWorks

 475 Wolf Ledges Parkway Akron, Ohio 44311

 virtualdataworks.com

 (330)800-2186

02 | WHY SECURING YOUR SOFTWARE SUPPLY CHAIN IS CRITICAL

In today's world, everything's connected. That includes the software your business relies on, whether you've installed that software locally or use it in the cloud.

Protecting the entire process that creates and delivers your software is very important. From the tools developers use to the way updates reach your computer, every step matters. A breach or vulnerability in any part of this chain can have severe consequences.

A recent example is the global IT outage that happened last July. This outage brought down airlines, banks, and many other businesses. The culprit for the outage was an update gone wrong. This update came from a software supplier called CrowdStrike. It turns out that the company was a link in a LOT of software supply chains.

What can you do to avoid a similar supply chain-related issue? Let's talk about why securing your software supply chain is absolutely essential.

Increasing Complexity and Interdependence

• Many Components

These include open-source libraries, third-party APIs, and cloud services. Each component introduces potential vulnerabilities.

• Interconnected Systems

A vulnerability in one part of the supply chain can affect many systems. The interdependence means that a single weak link can cause widespread issues.

• Continuous Integration and Deployment.

Securing the CI/ CD pipeline is crucial to prevent the introduction of malicious code.

Rise of Cyber Threats

• Targeted Attacks

Attackers infiltrate trusted software to gain access to wider networks.

• Sophisticated Techniques

These include advanced malware, zero-day exploits, and social engineering. A robust security posture is necessary to defend against these threats.

• Financial and Reputational Damage

Companies may face regulatory fines, legal costs, and loss of customer trust. Recovering from a breach can be a lengthy and expensive process. Regulatory Requirements

• Compliance Standards

These include regulations like GDPR, HIPAA, and the Cybersecurity Maturity Model Certification (CMMC).

• Vendor Risk Management

Companies must ensure that their suppliers adhere to security best practices. A secure supply chain involves verifying that all partners meet compliance standards.

• Data Protection

Securing the supply chain helps protect sensitive data from unauthorized access. This is especially important for industries like finance and healthcare.

Ensuring Business Continuity

• Preventing Disruptions

A secure supply chain helps prevent disruptions in business operations as cyber-attacks can lead to downtime.

• Maintaining Trust

By securing the supply chain, companies can maintain the trust of their stakeholders.

Steps to Secure Your Software Supply Chain

• Strong Authentication

Use strong authentication methods for all components of the supply chain. Ensure that only authorized personnel can access critical systems and data.

• Phased Update Rollouts.

Keep all software components up to date, but don't do all systems at once. If those systems aren't negatively affected, then roll out the update more widely.

• Security Audits

Assess the security measures of all vendors and partners. Identify and address any weaknesses or gaps in security practices.

• Secure Development Practices

Ensure that security is integrated into the development lifecycle from the start.

• Threat Monitoring

Use tools like intrusion detection systems (IDS) as well as security information and event management (SIEM) systems.

• Education

Awareness and training help ensure that everyone understands their role in maintaining security.

A breach or outage can have severe consequences. Securing your software supply chain is no longer optional; investing in this is crucial for the resilience of any business.



Our complimentary network assessment thoroughly evaluates your IT infrastructure at no cost, identifying vulnerabilities, performance bottlenecks, and areas for improvement. It enhances security by addressing gaps, optimizes network efficiency, and reduces costs by eliminating unnecessary expenses. You'll also receive expert recommendations for future growth and scalability. Ensure your network is robust, secure, and ready for the future with this valuable service.

REQUEST YOURS ASSESSMENT 

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:

1. **Identify and Prioritize:** Focus on the most critical issues that will drive the most value first. This ensures that your efforts are directed where they can make the most significant impact.
2. **Integrate Debt Management into Your Workflow:** Maintain a balance between new development and debt reduction. This approach helps in managing technical debt without stalling progress on new features.

3. **Educate and Train Your Team:** Foster a culture of quality thinking. Continuous education and training ensure that your team is aware of best practices and the importance of addressing technical debt.

4. **Improve Documentation:** Good documentation provides a reference for current and future team members, making it easier to understand and manage the system.

5. **Regularly Update and Refactor Systems:** This involves making small, manageable changes to improve quality. Regular updates and refactoring help in keeping the system robust and adaptable.

6. **Optimize Security Practices:** Maintaining strong security practices helps ensure system reliability and performance. Regular security audits and updates are crucial.

7. **Manage Dependencies:** Tracking dependencies ensures compatibility and security. Keeping an eye on dependencies helps in avoiding unexpected issues and vulnerabilities.

8. **Foster a Culture of Continuous Improvement:** Encourage learning, celebrate successes, and engage in regular reflection to drive ongoing enhancement. This culture promotes a proactive approach to managing technical debt and improving the system.

By systematically addressing technical debt, you enhance the long-term health and performance of your IT systems, ensuring they remain efficient, secure, and scalable. This approach reduces maintenance costs, improves system performance, and mitigates security risks. Prioritizing critical issues, integrating debt management into workflows, and fostering a culture of quality and continuous improvement are key. Regular updates, improved documentation, optimized security practices, and managing dependencies further strengthen your systems, making them resilient and adaptable to future demands.

04 ENHANCING EMPLOYEE PERFORMANCE WITH A MOBILE-OPTIMIZED WORKSPACE

Today’s workspaces transcend physical boundaries. Employees work and collaborate seamlessly from anywhere, whether they’re sipping coffee at a local café or lounging on their living room couch. That’s the magic of a mobile-optimized workspace. It’s a game-changer for productivity and performance.

Core Components of a Mobile-Optimized Workspace

- **Cloud-Based Everything.** This ensures seamless access to files, applications, and collaboration tools from any device.
- **Mobile-First Applications.** Ensure they are intuitive, responsive, and offer the same functionality as desktop versions.
- **Robust Collaboration Tools.** Features like real-time editing, file sharing, and video conferencing are essential.
- **Secure Mobile Device Management.** Protect sensitive company data on mobile devices.
- **Employee Training.** Equip employees with skills to effectively use mobile devices for work.

Benefits of a Mobile-Optimized Workspace

- Increased Productivity
- Enhanced Collaboration
- Improved Decision Making
- Attracting Top Talent
- Cost Savings

Challenges and Considerations

While the benefits are clear, creating a mobile-optimized workspace isn’t without challenges.

- **Security Risks:** Increased device usage means a larger attack surface. Put in place robust security measures to protect sensitive data.
- **Employee Distractions:** Encourage employees to use focus modes or apps to reduce interruptions.
- **Data Usage:** Be mindful of data consumption. Consider providing mobile hotspots or Wi-Fi allowances.
- **Device Management:** Consider using mobile device management (MDM) solutions to streamline the process.

05 6 TIPS TO TROUBLESHOOT COMMON BUSINESS NETWORK ISSUES

Get started on keeping your network up and running smoothly:

1. **Identify the Problem**
Narrow down potential causes.
2. **Inspect Physical Connections**
Quickly rule out or identify simple problems.
3. **Test Network Connectivity**
Simple testing can provide valuable insights.
4. **Analyze Network Configuration**
Errors here can often cause connectivity problems.
5. **Monitor Network Performance**
This helps identify ongoing issues and potential bottlenecks.
6. **Ensure Security and Updates**
Regular updates and checks can prevent many common issues.

06 COMMON MOBILE MALWARE TRAPS

Mobile malware is often overlooked. People focus on securing their laptops or desktops without paying close attention to smartphone and tablet security. Mobile malware can arrive in various forms, from sneaky apps to deceptive links. Ignorance is not bliss here. Understanding the common traps is your first line of defense.

- **Phishing Attacks**
Clicking links or downloading attachments can lead to malware infection.
- **Malicious Apps**
Always research apps before downloading.
- **SMS Scams**
Be wary of unexpected messages, especially those asking for sensitive info.
- **Public Wi-Fi networks**
Avoid accessing sensitive information on public Wi-Fi.
- **Fake Apps**
Always verify app authenticity
- **Adware**
Less harmful but can be annoying and can expose you to other threats.

07 WHAT IS A PASSWORD MANAGER AND WHY IS IT USEFUL?

A password manager is a software application designed to store and manage online credentials. It securely saves passwords and other login information in an encrypted database, which can be accessed with a single master password.

This tool is highly useful as it helps users generate strong, unique passwords for each of their accounts, reducing the risk of security breaches caused by weak or reused passwords. Additionally, it simplifies the login process by automatically filling in credentials, saving time and effort while enhancing overall security.

READ MORE





CHECK OUT OUR MONTHLY TECH BYTE NEWSLETTERS!

Our Tech Byte Newsletters are monthly publications that provide updates on technology and cybersecurity news. They cover a range of topics, including the latest trends in cyber threats, strategies for leveraging technology to enhance business operations, and insights into cybersecurity practices. Each edition aims to keep readers informed about the evolving tech landscape and offers practical tips to help businesses stay secure and efficient.

[READ MORE](#)

