onestep
Secure IT Services

VOL. 4 | 2024

THE LATEST BYTE
CYBERSECURITY REFRESH

Back to the Basics

As we all prepare to leap into a new year, *The Latest Byte* is hitting the reset button...

...and returning to the cybersecurity basics

Think of it as a digital cleaning—minus the dust bunnies. We've got your ultimate check-list to see if your online defenses are up to snuff, and we'll dive into recent hacks to uncover which security slip-ups made headlines.

Join us for a fun and informative journey as we sharpen our cyber-savvy skills and prepare to face whatever your business technology throws our way. Stay sharp, stay secure, and let's make this coming year the safest one yet!

ABOUT ONE STEP SECURE IT

We are an outsourced IT company

with over three decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

One Step's expertise includes Cybersecurity, Managed IT and Co-Managed IT, Information Security, and Compliance Services. We understand that as business operations evolve, so do the security threats. Our expert team collaborates closely with you to create a customized IT strategy, identify vulnerabilities, and strengthen your IT infrastructure.

Our corporate headquarters are in Phoenix, Arizona, and we proudly serve businesses nationwide. Ready to take your business to the next level? Find out how One Step can increase employee productivity and make your business more secure. Visit us at **www.onestepsecureit.com** to learn more.

Meet One Step's CEO & Founder
Scott Kreisberg

Scan the QR code.

Revamping Business Security Essentials Before the New Year

Cybersecurity isn't just essential; it's a cornerstone of business resilience. Overlooking basic cybersecurity measures can leave businesses vulnerable to serious risks, including data breaches, operational disruptions, and potential regulatory fines.

On the next page, let's review the cybersecurity basics companies often overlook, yet they can have a profound impact when properly implemented.

01 Employee Training & Awareness

Impact when neglected: Untrained employees are more likely to fall victim to phishing scams or unknowingly download malware, leading to compromised systems and data leaks.

Building defense: Regular training on cybersecurity best practices empowers employees to recognize and report threats, creating a human firewall against cyber attacks.

02 Regular Software Updates & Patch Management

Impact when neglected: Outdated software and unpatched systems are vulnerable to exploits and vulnerabilities, making them easy targets for cyber criminals.

Building defense: Establish a patch management process by identifying critical assets, prioritizing updates, and scheduling regular patches.

03 Strong Password Policies & Multi-Factor Authentication

Impact when neglected: Weak passwords and lack of MFA leave accounts susceptible to brute-force attacks and unauthorized access.

Building defense: Enforcing complex password requirements and implementing MFA adds layers of security, significantly reducing the risk of unauthorized access to systems and data.

04 Data Backup & Recovery Plans

Impact when neglected: Failure to back up critical data regularly can result in devastating data loss during ransomware attacks or hardware failures.

Building defense: Automate backups, store them securely offsite, and routinely test recovery plans to ensure business continuity and resilience against data loss incidents.

05 Access Control & Principle of Least Privilege

Impact when neglected: Poorly managed user permissions increase the risk of insider threats and unauthorized access to sensitive information.

Building defense: Enforce strict access controls by using role-based permissions, regularly reviewing access rights, and applying the principle of least privilege to limit user access and reduce the attack surface.

06 Mobile Device Security

Impact when neglected: Unsecured mobile devices accessing corporate networks can introduce malware or lead to data breaches.

Building defense: Enforcing mobile device management policies, such as device encryption and remote wipe capabilities, safeguards corporate data on mobile devices.

Businesses can establish a resilient foundation against evolving cyber threats by prioritizing these cybersecurity fundamentals. Implementing these measures not only mitigates risks but also enhances trust with customers and partners, positioning the organization for sustainable growth and success.

How to Get Employees to Care About Cybersecurity

Employee buy-in is crucial for any cybersecurity initiative to succeed. However, motivating employees to genuinely care about cybersecurity can be challenging. Here are practical strategies businesses can use to foster a culture where everyone takes cybersecurity seriously:

1. **Make Cybersecurity Personal** Employees often view cybersecurity as something that only concerns the IT department. By framing it in a way that shows how it protects not just the business but also their personal data, you can create a more relatable connection.

2. **Provide Clear Communication and Practical Examples** Avoid overwhelming employees with jargon. Use clear, straightforward language and provide practical examples of how small actions—like clicking on a suspicious link—can lead to massive consequences for the entire organization. Sharing real-life stories of companies that suffered from cyber incidents can help employees see the tangible impact of their role in cybersecurity.

3. **Lead by Example from the Top Down** When leadership visibly prioritizes cybersecurity and follows best practices themselves, it sets a powerful precedent. Leaders who actively engage in cybersecurity training and encourage open conversations about potential threats help to embed a security-first mindset throughout the organization.

4. **Give Regular, Bite-Sized Updates and Reminders** Instead of overwhelming employees with information all at once, share bite-sized tips and reminders regularly. Quick tips in newsletters, posters around the office, or short reminder emails can keep cybersecurity top of mind without becoming tedious.

5. **Tie Cybersecurity to Business Success** Show employees how cybersecurity directly impacts the company's success and, by extension, their job security and career growth. Highlight how strong security practices protect the business from costly breaches, which allows for more resources to be allocated toward growth, innovation, and employee benefits.

6. **Create a Positive, No-Blame Culture** Employees are more likely to report suspicious activity or admit to mistakes if they know they won't be harshly penalized for it. By fostering a no-blame culture, which focuses on learning and improvement rather than punishment, businesses encourage proactive participation in cybersecurity practices.

When employees feel connected to the broader mission of protecting the organization, they're more likely to embrace cybersecurity as part of their everyday duties. By making security training engaging, relevant, and integrated into the company culture, businesses can transform their workforce into their first line of defense.

Preparing for Business Disruptions: Are Companies Ready?

Cyber threats are increasingly sophisticated, and businesses must be prepared for any potential disruptions. Third-party tools like CDK Global and cybersecurity firms like CrowdStrike have recently faced significant breaches that reveal vulnerabilities in even the most secure environments. These incidents underscore the need for robust infrastructure, thorough vendor assessments, and proactive security measures.

CDK Global Breach:
A Case of Third-Party Risk

Earlier this year, CDK Global, a major IT service provider for the automotive industry, suffered a breach that compromised sensitive customer and vehicle data.

How it happend?

Attackers initially gained access through a compromised third-party vendor with weak security controls, allowing them to infiltrate CDK's systems.

Lateral Movement & Data Exfiltration

Once inside, attackers moved through the network, escalated privileges, and exfiltrated sensitive data without detection.

Response & Mitigation

The breach was detected only after unusual activity was observed. CDK responded by enhancing third-party security assessments, tightening access controls, and improving monitoring.

This breach highlights the critical importance of securing third-party vendors and maintaining strong internal security defenses.

CrowdStrike Incident:
The Risks of Phishing and Internal Vulnerabilities

In mid-2024, CrowdStrike, a leading cybersecurity firm, experienced a significant breach that exposed sensitive client information.

How it happend?

The breach began with a sophisticated phishing campaign that tricked employees into revealing credentials, which attackers then used to bypass security and infiltrate the network.

Lateral Movement & Data Exfiltration

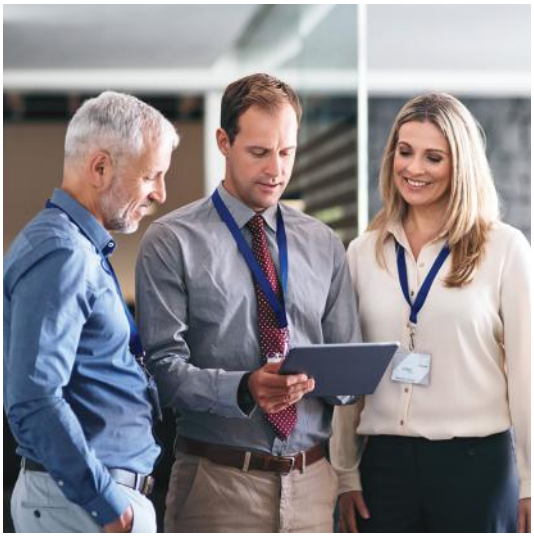
Attackers escalated their access, moved laterally through the network, and exfiltrated client data and proprietary intelligence, evading detection for some time.

Response & Mitigation

CrowdStrike detected the breach through anomaly monitoring and responded by containing the breach, strengthening employee training, and bolstering internal security protocols.

This incident underscores the necessity of ongoing employee training and the importance of rigorous internal security measures, even for companies that specialize in cybersecurity.

These examples serve as a reminder that even the most well-prepared businesses can face significant risks if their infrastructure, third-party relationships, and internal practices are not thoroughly secured. By understanding these vulnerabilities and learning from past incidents, companies can better prepare for potential disruptions and strengthen their defenses against future threats.



Read how you can strengthen your organization's defenses with risk management tools.

Scan the QR code to start reading or visit our One Step Secure IT Blog at :

www.onestepsecureit.com/blog/strengthening-defenses-exploring-cybersecurity-risk-management-tools

Security for Businesses: Protecting Against Cyber Attacks

Businesses must invest in proactive defenses and have a solid after-breach action plan in place. A comprehensive action plan allows for swift containment, detailed investigation, and clear communication following an attack. By being prepared, companies can reduce financial losses, limit reputational damage, and recover more effectively from a breach.

Steps SMBs Should Take After a Cyber Attack

written by Brett Stoddard

Meet Brett Stoddard...

Brett Stoddard is a technology executive with over 25 years of experience. His journey began after earning a Bachelor of Business Administration from Idaho State University. He then joined the Federal Bureau of Investigation, where he contributed to national security and technological advancements. Today, as the Chief Operating Officer at One Step Secure IT, Brett Stoddard focuses on driving data security and technological innovation.

Following a cyber attack or breach, Mr. Stoddard recommends the following concise steps for a small to medium-sized business (SMB) to take:

1. IMMEDIATE CONTAINMENT

Disconnect Affected Systems: Unplug compromised computers and servers from the network.

Preserve Evidence: Avoid turning off systems; document all actions taken.

2. ENGAGE INCIDENT RESPONSE TEAM

Notify IT Team: Alert your internal IT team or managed service provider.

Notify Insurance Carrier: If you have cyber insurance, contact the incident response hotline.

Contact Experts: Engage cybersecurity professionals if at hand.

3. INITIAL ASSESSMENT

Determine Scope: Identify affected systems and data.

Identify Attack Vector: Understand how the breach occurred.

4. COMMUNICATION

Internal Notification: Inform senior management and relevant teams.

External Notification: Prepare communication for customers and stakeholders if necessary.

5. INVESTIGATION

Collect Evidence: Secure logs and take system images.

Identify Malicious Activity: Look for indicators of compromise.

6. ERADICATION AND RECOVERY

Remove Threats: Eliminate malware and close back-doors.

Patch Vulnerabilities: Apply necessary updates.

Restore Systems: Use clean backups to restore data.

7. POST-INCIDENT REVIEW

Analyze Incident: Conduct a post-mortem to understand the breach and response.

Update Policies: Revise security policies and response plans.

8. ENHANCE SECURITY MEASURES

Strengthen Controls: Implement firewalls, IDS, MFA, and encryption.

Employee Training: Conduct regular cybersecurity training.

9. CONTINUOUS MONITORING

Monitor Systems: Implement ongoing monitoring for suspicious activity.

Regular Audits: Perform security audits and vulnerability assessments.

For more insights, check out Brett's appearance on the *One Step Beyond Cyber* Podcast hosted by CEO and Founder of One Step Secure IT, Scott Kreisberg.

Listen to Brett Stoddard on

ONE STEP BEYOND CYBER

PODCAST

Drawing from years of experience, Brett dives into real-world stories and offers practical tips to help businesses stay ahead of today's most pressing cyber threats.

Scan QR Code below to start listening to *Balancing Security and Efficiency: Insights from Brett Stoddard*

10 KEY CYBER SAFETY TIPS

Even the most fundamental cybersecurity practices can sometimes be overlooked. Yet, these simple actions often play a crucial role in safeguarding our personal and professional lives.

Are you staying current with these essential 10 cyber safety tips?

1
Set up separate email accounts for work, personal use, alerts, and other interests.

2
Exercise caution when clicking on links or attachments in emails or text messages.

3
Use secure messaging tools for transmitting sensitive information.

4
Create and regularly update strong passwords.

5
Avoid using the same password across multiple accounts.

6
Minimize the use of unsecured public networks.

7
Limit web usage at work to essential, business-related sites.

8
At home, establish a primary network and a separate one for guests, children, and smart devices.

9
Install and keep anti-virus software updated on all devices.

10
Be mindful of sharing information on social media regarding yourself, your family, your job, or your business.

DIGITAL LIBRARY

One Step Secure IT's Digital Library offers access to a range of resources designed to enhance your IT, cybersecurity, and business technology knowledge. Get a digital copy of our in-depth resources and stay informed about the best practices for optimizing and protecting your business.

TAME THE TECH BEAST

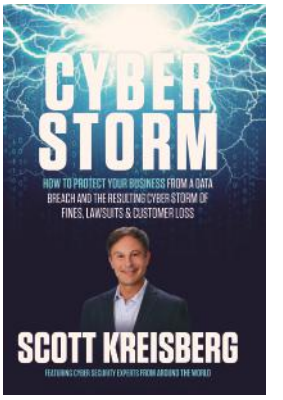
A business owners' practical guide to finding reliable and trustworthy IT support to reduce technology costs, minimize cyber threats, and increase employee productivity.

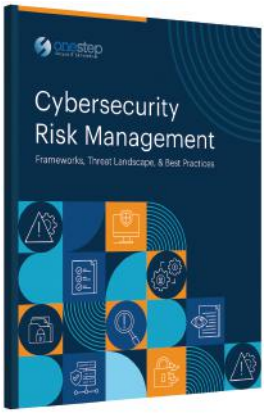
Scan QR Code to Download >>>

CYBER STORM

Cyber Storm offers business owners insight into the tactics they can use to protect themselves from data breaches and the resulting "cyber storm" of fines, lawsuits, and customer loss.

Scan QR Code to Download >>>





CYBERSECURITY RISK MANAGEMENT:

Frameworks, Threat Landscape, & Best Practices

This eBook is an essential guide to managing the risks created by increasing cyber attacks, safeguarding business operations, and protecting your reputation and sensitive data.

Scan QR Code to Download >>>

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027

onestep
Secure IT Services

www.OneStepSecureIT.com | (623) 227-1997

Connect with us @OneStepSecureIT