

THE CYBERSIDE BRIEF

Insider Wisdom from 20 Years of IT Defense for Your Business Prosperity and Security

INSIDE THIS ISSUE

What Do You Do When A Company Compromises Your Data? **P. 1**

FREE Audit: Free Cyber Security Audit Will Reveal Where Vulnerabilities Are And How To Protect Your Business **P. 2**

COMPLIANCY NAVIGATOR: Must Pen Testing And Vulnerability Scanning Be Done To FedRAMP Standards For CMMC Compliance? *By Patrick Birt* **P. 3**

Are You Using This Helpful Google Calendar Hack? **P. 4**

SAFE CYBER SPOTLIGHT: Beware Of QR Code Phishing Scams **P. 4**

Notable Team Achievements: Congratulations Evan **P. 4**

Mike Michalowicz Explains How To Build A Team That Cares About Your Company's Success As Much As You Do **P. 5**

Don't Make This Mistake With Your Home's Smart Tech **P. 6**

This monthly publication is provided courtesy of Patrick Birt, President of AdRem Systems Corporation.



WHAT DO YOU DO WHEN A COMPANY COMPROMISES YOUR DATA?

With the rise in cyber-attacks worldwide, you've likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can't control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers' personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, SSNs, etc. – the most commonly breached type of data. A recent

example is ChangeHealthcare, breached in February of this year. Due to the breach, it's estimated that one-third of Americans – possibly including you – had sensitive information leaked onto the dark web.

So now what? What do you do when you receive a letter in the mail from your health care provider or favorite retail store admitting, "Whoops, we got breached." It's more than upsetting to think that your data is now in the hands of criminals. When sensitive information leaks, you'll have to do some recon to protect your

continued on page 2...

...continued from cover

accounts from suspicious activity. Follow these seven steps to stop the bleeding after a company fails to protect your data from being compromised.

What To Do After Your Data's Been Leaked

1. First, make sure the breach is legit.

One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

2. Figure out what data was stolen.

After speaking directly with the company, determine what data was stolen. Credit cards can be easily replaced; Social Security numbers, not so much. You'll want to know what was

compromised so you can take the necessary steps to monitor or update that information.

3. Change passwords and turn on MFA.

After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.

While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

4. Monitor your accounts.

Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorize. They may be a sign of identity theft. If your credit card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

5. Report it.

If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like

local law enforcement or the Federal Trade Commission. They can provide guidance and next steps on how to protect your identity.

6. Be aware of phishing attempts.

Often, after data leaks, hackers use the information about you they stole to send you phishing e-mails or calls to trick you into giving away even more sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

7. Consider identity theft and data breach protection.

Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your SSN. It's a time-consuming process to replace a Social Security card. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimize a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an increasingly risky digital world.

FREE CYBER SECURITY AUDIT:

FREE Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.



To Get Started And Claim Your FREE Assessment Now:

Call Our Office At (703) 860-2233
or Scan QR Code





MUST PEN TESTING AND VULNERABILITY SCANNING BE DONE TO FedRAMP STANDARDS FOR CMMC Compliance?

Compliance Navigator



In the journey towards CMMC compliance, understanding the nuances between Penetration Testing and Vulnerability Scanning is essential. While these terms are often used interchangeably, they represent different aspects of a cybersecurity strategy. This article aims to clarify their definitions, pinpoint where they fit within the frameworks of NIST SP 800-171 and CMMC, and address whether these activities need to meet FedRAMP standards.

PENETRATION TESTING VS VULNERABILITY SCANNING

Penetration Testing involves simulating cyberattacks on a system to identify exploitable vulnerabilities. It goes beyond surface-level assessments to see how deep an attacker can penetrate your defenses. – Like having a hacker on your network. Vulnerability Scanning, on the other hand, is an automated process that scans systems for known vulnerabilities and provides a report on potential exposures. It is more about identifying risks rather than exploiting them.

NIST SP 800-171 REQUIREMENTS

NIST SP 800-171 outlines the security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems. While it emphasizes regular monitoring and risk assessments, it does not explicitly mandate Penetration Testing. Instead, it focuses on:

- 3.11.1: Periodically assess the security controls in organizational systems to determine if the controls are effective.
- 3.11.2: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities.

Penetration Testing is implied as a part of these assessments but is not specifically required.

CMMC REQUIREMENTS

CMMC Level 1:

- Primarily focuses on the protection of Federal Contract Information (FCI).
- Does not explicitly require Penetration Testing or Vulnerability Scanning.
- Emphasizes basic safeguarding requirements and procedures.

CMMC Level 2:

- Primarily focuses on the protection of CUI
- While not mandating Penetration Testing, it introduces more rigorous monitoring and scanning practices.
- Domain: Risk Management (RM) highlights continuous monitoring and identifying vulnerabilities.
- Security Assessment (CA) emphasizes the implementation and continuous monitoring of security controls, including vulnerability scanning, to ensure and maintain the organization's security posture.

CMMC Level 3:

- Implies more advanced security measures, including regular assessments and possibly Penetration Testing.
- Practice: CA.3.162 mentions employing security assessments to validate the effectiveness of security measures, which can include Penetration Testing.

FedRAMP STANDARDS

FedRAMP (Federal Risk and Authorization Management Program) provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies. While CMMC and FedRAMP are separate frameworks, there are overlaps in the security controls and requirements they impose.

For CMMC Level 2 systems, which handle CUI, adhering to high security standards is crucial. While CMMC itself does not explicitly mandate that Penetration Testing and Vulnerability Scanning meet FedRAMP standards, aligning with these standards can provide additional assurance of the security posture, especially when dealing with federal contracts.

USING THIRD-PARTY VENDORS

When choosing third-party vendors for Penetration Testing or Vulnerability Scanning on systems that handle CUI, the following considerations are important:

1. Accreditation and Expertise: Ensure that the third-party vendor has relevant experience and credentials, such as certifications in cybersecurity and compliance standards (e.g., ISO 27001, CSSP, CEH).
2. Compliance with CMMC Requirements: The vendor should be familiar with CMMC requirements and the specific needs of handling CUI. This ensures that their testing methodologies align with the required security controls.
3. FedRAMP Authorized Vendors: While not mandatory, using FedRAMP authorized vendors can provide additional assurance that the vendor meets stringent federal security standards. This is particularly relevant if your organization also deals with FedRAMP-authorized systems or seeks a higher level of security assurance.

RECOMMENDATIONS

1. Due Diligence: Conduct thorough due diligence when selecting a vendor. Review their credentials, past performance, and understanding of CMMC and NIST SP 800-171 requirements.
2. Alignment with Security Controls: Ensure that the testing procedures align with the security controls and risk management practices outlined in CMMC Level 2.
3. Continuous Monitoring: Implement continuous monitoring and regular assessments, including vulnerability scans, to maintain compliance and security over time.
 - a. Note: While neither NIST SP 800-53 nor NIST SP 800-171 explicitly state

continued on page 4...

ARE YOU USING THIS HELPFUL GOOGLE CALENDAR HACK?

It's a bit embarrassing when you log in to your computer at 9:00 a.m. only to realize you missed the all-team Zoom



meeting at 8:30 a.m. Thankfully, Google Calendar offers a helpful hack: daily agendas. With this feature, you can send yourself a daily agenda first thing in the morning so you know everything planned for the day.

To set it up, log into your Google account and go to Settings. Find "Settings for my calendars" > "Other notifications" > "Daily agenda." The default is set to "None," so click on it and change it to "Email." Now you have a daily agenda automatically sent to your inbox before you even get out of bed!

CARTOON OF THE MONTH



"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back and you're going to say you're sorry."

...continued from page 3

"yearly penetration tests" or "monthly vulnerability scanning," the following recommendations are commonly derived from these standards and industry practices.

Yearly Penetration Testing:
Recommended by NIST SP 800-53 control CA-8 and aligned with industry best practices.

Monthly Vulnerability Scanning:
Recommended by NIST SP 800-53 control RA-5 and NIST SP 800-171 control 3.1.2, aligning with regular and continuous monitoring best practices.

CONCLUSION

Understanding the distinction between Penetration Testing and Vulnerability Scanning, and their roles within the NIST SP 800-171 and CMMC frameworks, is crucial for achieving and

maintaining compliance. While not always mandatory, these practices play a vital role in a robust cybersecurity program. By integrating both into your security strategy, you can better protect sensitive information and meet the evolving requirements of CMMC compliance.

At Sherpa, we offer Penetration Testing and Vulnerability Scanning services that align with FedRAMP standards, helping to bolster your security posture and ensure your systems handling CUI are secure and well-managed. Contact us today to learn more about how our services can support your compliance and security needs.

SPONSERED BY SHERPA, AN ADREM SYSTEMS COMPANY:



theSherpa.us | 571-360-3926 | info@thesherpa.co

Patrick Birt is the Owner and CEO of AdRem Systems Corporation and Compliancy Sherpa, LLC. He uses over 35 years of IT and federal service experience as a Lead Engineer for government solutions to guide organizations in safeguarding sensitive data against cyber threats. His deep understanding ensures strategies align and empower businesses with the complex compliance and technology needs of Today.



Congratulations EVAN MARTEL

NOTABLE TEAM ACHIEVEMENTS

We're thrilled to recognize one of our dedicated technicians, Evan Martel, for his recent accomplishments in advancing his technical expertise!

Evan has successfully completed a series of rigorous vendor certifications, including those in remote monitoring and management, IT documentation, professional services automation, and networking. His achievement as an expert in these areas reflects our team's ongoing commitment to excellence and our dedication to delivering the highest quality service to our clients. Congratulations, Evan, on your hard work and dedication!



SAFE CYBER SPOTLIGHT

BEWARE OF QR CODE PHISHING SCAMS



While QR codes provide a lot of ease and efficiency for businesses to advertise their products or services, they also present a new avenue for scammers. Educate your employees about QR code phishing scams and how to avoid them.



MICHAEL MICHALOWICZ

EXPLAINS HOW TO BUILD A TEAM THAT CARES ABOUT YOUR COMPANY'S SUCCESS AS MUCH AS YOU DO



Early in his career, Mike Michalowicz was eager to announce to his team a new corporate vision for the year: a \$10 million revenue goal. However, what he imagined would be one of his greatest visionary moments as a leader was one of his biggest mistakes.

After revealing the vision to his team, “it was total silence,” Michalowicz explained to a room of business leaders at a recent industry conference. “A colleague came over to me and said, ‘Mike, if we achieve \$10 million in revenue, you get the bigger house. You get the new car. That’s your vision. What about our vision?’” This was a transformative learning moment for Michalowicz, who committed himself to learning what it takes to be a GREAT leader.

Today, Michalowicz is the author of several books, including *Profit First*, *Get Different*, *The Pumpkin Plan* and other small business must-reads. He’s an entrepreneur and speaker teaching other leaders how to build and retain unstoppable teams who care about the company’s success as much as you do, so you’ll be happier, grow faster and create an environment where everyone flourishes.

How To Build An Unstoppable Team

1. Most leaders tell their team what to do. Great leaders ask their team what they could do. One of the Baltimore Museum of Art’s most successful exhibits was curated by 17 museum guards. The idea came from a conversation between a curator and a guard around what the guard did day-to-day. He revealed how much he learned about the art from patrons and what interested them. Museum leaders quickly learned this wasn’t unique to the one guard, and a group was assembled to create “Guarding the Art.” Michalowicz explains that great leaders encourage ownership by asking, “What could we do?” rather than always telling their employees what to do.

2. Great leadership assembles and unifies.

The movie *The Boys in the Boat* recounts how an inexperienced US rowing team won gold in the 1936 Olympics. The leader helped the team connect, communicate and work together to win against all odds. He fostered deep trust within the team, which Michalowicz says distinguishes great leadership in any circumstance.

3. Great leaders follow a FASO model.

Michalowicz’s research and experience in leadership culminate in a four-part model he calls “FASO.” Leaders who want to be great can use FASO to assemble an unstoppable team.

- **F – “Fit.”** When hiring a new team member, they must be an ideal fit for the organization, and the organization must be an ideal fit for them.
- **A – “Ability.”** Great leaders look for people’s raw potential. Do they have curiosity, desire and a thirst for the role? That’s what great leaders hire and recruit for, not simply experience and innate ability.
- **S – “Safety.”** Great leaders account for their team’s physical, relational and financial safety. They ensure that people feel safe in how they are treated and where they work, they have a transparent financial culture and they educate their team on personal finances.
- **O – “Ownership.”** “When we’re forced to comply, we’ll seek to defy,” Michalowicz says. Great leaders encourage their team to personalize, gain intimate knowledge of and control aspects of their work.

Above all, Michalowicz says, “No one cares how you care; they care THAT you care.” Show your team you care by working to incorporate these great leadership approaches in your organization.

OUR SERVICES

IT BUSINESS SOLUTIONS

Managed and Co-Managed Service (MSP)
 Managed Security Service (MSSP)
 Cloud Computing
 VoIP Solutions
 Data Backup and Recovery
 Cybersecurity
 Vendor Management
 Hardware as a Service (HaaS)
 Secure Access Service Edge (SASE)
 Virtualization
 Remote Work Environments

COMPLIANCE SOLUTIONS

CMMC, NIST, HIPAA, ISO, FTC,
 etc.
 Email Enclaves
 Employee Security Training
 Data Backup and Recovery
 Data Privacy and Encryption
 Disaster Recovery Planning
 Penetration Testing
 Vulnerability Scanning
 Policy Consulting
 Cybersecurity Consulting

HARDWARE PROCUREMENT

Shop.AdRem.com

HOSTING & ONLINE SERVICES

OnlineServices.AdRem.com

Domain Registration and Transfer
 Website Hosting: Website Builder &
 WordPress
 Website Security Solutions
 Custom Website Design
 WordPress Website Support Solutions
 Logo Design
 Virtual Private Servers (VPS)
 Dedicated Servers
 Email Marketing



OUR MISSION

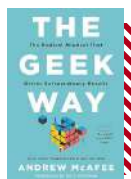
To apply our 20 Year Legacy of knowledge and innovation, to defend Critical IT Networks, and encourage a more secure nation of Tomorrow by delivering Today's technologies with respected, trusted, and proven individuals.

THE GEEK WAY:

The Radical Mindset That Drives Extraordinary Results

By Andrew McAfee

When we have a big problem, we like to go to experts who don't just like what they do but are downright geeky about it. Geeks are known for being intelligent and efficient problem-solvers, but what if we could all benefit from a geeky mindset to perform better in our work and lives?



In *The Geek Way: The Radical Mindset That Drives Extraordinary Results*, Andrew McAfee explores four "norms" – science, ownership, speed and openness – that define geek culture. He explains that when these norms are aligned, it taps into our human superpowers: our ability to cooperate intensely and learn quickly. This book blends science, history and real-world examples to provide insights into harnessing geek culture for innovation. *The Geek Way* is a compelling read for anyone interested in channeling their inner geek to improve their ideas, business or community.

DON'T MAKE THIS MISTAKE WITH YOUR HOME'S SMART TECH

Smart devices are so pervasive throughout our homes that it's hard to imagine what life was like before them. From door cams that show us when our kids get home to AI-powered devices that keep track of grocery lists and play our favorite music while we cook, we truly live in "smart" homes.

But unlike devices of the past, you can't "set and forget" smart devices. These tools are connected to the Internet, where hackers keep a close eye out for unprotected devices.

When they find a device with a weak password, they can access it and carry out terrifying crimes like watching your family through a home camera. Before you plug in your smart device, follow these simple steps to make sure it's not an open door for peering eyes.

Pros And Cons Of Smart Devices

When hackers find an unprotected device – like an indoor cam that you never bothered to change the default password to – they can access sensitive information on your account, including your address, birth date, e-mail address and phone number. Criminals use this information to create a profile about you and carry out targeted attacks. A family in Mississippi even had a hacker taunt their young daughter through their Ring camera.

Thankfully, you can take a few simple security steps to avoid becoming a victim of your smart device.

Steps To Keep Your Smart Home Safe

1. Change the default login information immediately. Default passwords are low-hanging fruit for hackers, so be sure to change this to a new, stronger password right away.
2. **Make sure your WiFi is secure.** If your WiFi password is a few years old or you use the same password on other accounts, change it to a stronger password.
3. **Enable multifactor authentication (MFA) in security settings.** This way, users can only log in with a security code or authenticator app, making it nearly impossible for hackers to get in.
4. **Regularly update the device.** Updates fix issues or add new features that may improve your security. Don't skip these updates. If your smart device doesn't update automatically, set a reminder in your phone to check for updates periodically.
5. **Consider separate networks.** Many WiFi providers offer guest networks. Consider connecting smart devices to a home guest network separate from the one that your phones or laptops are on. This way, if a smart device is hacked, it's not a straight shot to devices holding more valuable information.

The biggest mistake smart-device users make is thinking they can plug in their devices and walk away. These tips go a long way toward ensuring that your device isn't an open door to creepy criminals.

