THE CYBERSIDE BRIEF

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

SEASON'S GREETINGS

As the season of gratitude and celebration unfolds, we want to take a moment to thank our incredible clients and loyal newsletter subscribers. Your passion for growth and excellence inspires everything we do.

From the insights you share to the goals you achieve, your drive reminds us why we're dedicated to empowering leaders, managers, and business professionals like you. Each edition of our newsletter is crafted with care, aiming to provide you with valuable tools and knowledge to support your journey.

May the season bring you and your loved ones peace, joy, and renewed inspiration for the year ahead. Thank you for being a part of our community and allowing us to be a part of your success story.

Warm holiday wishes from all of us at AdRem Systems Corporation!

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

OUR MISSION:

To leverage over two decades of expertise and innovation to defend critical IT networks and foster a more secure nation of Tomorrow by delivering Today's technologies through a team of respected, trusted, and proven professionals.

THIS YEAR'S BIGGEST DATA BREACHES

According to *TechCrunch*, this year has seen some of the most damaging data breaches in history. In 2024 alone, hackers stole billions of personal records, and it's almost guaranteed your data is among those stolen records. Let's look at this year's record-breaking attacks and what you need to know about protecting your information.

1 National Public Data
(2 Billion-Plus Records)

What happened: In December 2023, hackers accessed the systems of National Public Data, a background-check company. In April, 2.7 billion records with highly sensitive data for 170 million people were leaked onto the dark web.

Who is exposed: The stolen data includes records for people in the US, Canada and the UK.

Compromised data: 2 billion-plus records containing full names, current and past addresses, Social Security numbers, dates of birth and phone numbers.

2 Change Healthcare
(38 Million Records)

What happened: In February, the UnitedHealth-owned tech firm Change Healthcare was hacked by a Russian ransomware gang that gained access through systems unprotected by multifactor authentication. The attack caused widespread downtime for health care institutions across the US and compromised data for many, many Americans.

continued on page 2...

...continued from cover

UnitedHealth paid $22 million to prevent data leaks, but another hacker group claimed to still have some of the stolen Change Healthcare data.

Who is exposed: Estimated data exposure for one-third of the American population (likely more).

Compromised data: Payment information, Social Security numbers and medical data, including test results, diagnoses and images.

3 AT&T
(Hacked TWICE)

What happened: In March, hackers released data for more than 73 million past and existing AT&T customers going back to 2019. Then, in July, data was stolen from an AT&T account the company had with data giant Snowflake (more on that in a bit). Reportedly, AT&T paid a ransom to the hackers to delete the data. However, if this data is leaked, it could expose the data of anyone called by AT&T customers, including noncustomers.

Who is exposed: 110 million-plus past and current customers and, potentially, noncustomers.

Compromised data: Personal information, including Social Security numbers and phone numbers.

4 Synnovis
(300 Million Patient Interactions)

What happened: In June, a UK pathology lab, Synnovis, was attacked by a Russian ransomware gang. The attack resulted in widespread outages in health institutions across London. Reportedly, Synnovis refused to pay the $50 million ransom.

Who is exposed: Past and existing patients in the UK.

Compromised data: 300 million patient interactions, including blood test results for HIV and cancer, going back many years.

5 Snowflake
(600 Million-Plus Recordings And Growing)

What happened: In May, cloud data giant Snowflake announced a system breach caused by stolen employee credentials. Hundreds of millions of customer records were stolen from Snowflake customers, including 560 million from Ticketmaster, 79 million from Advance Auto Parts and 30 million from TEG.

Who is exposed: Millions of customers from many of Snowflake's 165 corporate customers, including those mentioned above, plus Neiman Marcus, Santander Bank, Los Angeles Unified School District and many more.

Compromised data: Customer records.

How To Protect Yourself

You can't stop companies from getting hacked. However, you can prevent the situation from worsening for YOU by taking a few extra steps to protect your data. Here's what to do:

- **Review your health-related communications:** With so many breaches affecting health institutions this year, pay attention to your statement of benefits and look for services you didn't receive. If you spot something fishy, tell your health care provider and insurance company right away.
- **Freeze your credit:** This will stop criminals from opening a credit card or loan in your name.
- **Update your log-in credentials:** If you know what accounts were hacked, change your credentials, and also change the credentials to major accounts like your bank. Set up alerts too, so you're immediately aware of any unusual activity.
- **Be wary of e-mails:** After a breach, hackers access all kinds of information and may use that to send fraudulent e-mails. Slow down, read carefully and verify requests before taking any action.

Compliancy Navigator

PATRICK BIRT DETAILS WHAT THE NEW CMMC RULE MEANS FOR YOUR ORGANIZATION

On October 15, 2024, the Department of Defense (DoD) published the long-awaited final rule for the Cybersecurity Maturity Model Certification (CMMC) program, setting the stage for a new era of cybersecurity compliance. With this rule, critical timelines, levels of compliance, and the role of external service providers have been clarified, giving organizations a roadmap to align with federal cybersecurity requirement.

As the CMMC rule officially takes effect on December 16, 2024, it's important to understand what's changing and what's ahead.

UNDERSTANDING THE THREE LEVELS OF CMMC

The updated CMMC framework includes three levels, each tailored to the type of federal data your organization handles:

CMMC Level 1: Foundational

- **Who it applies to:** Contractors managing Federal Contract Information (FCI).
- **Requirements:** 17 basic cybersecurity practices from **FAR 52.204-21.**
- **Assessment:** Annual self-assessment, with results submitted to the Supplier Performance Risk System (SPRS).

CMMC Level 2: Advanced

- **Who it applies to:** Contractors handling Controlled Unclassified Information (CUI).
- **Requirements:** 110 security controls from NIST SP 800-171, addressing risks such as access control and incident response.
- **Assessment:**
  - 5% (Projected) of organizations will self-assess annually and submit results to SPRS.
  - 95% (Projected) of organizations will require a C3PAO (Certified Third-Party Assessor Organization) to assess compliance every three years, with results submitted to eMASS.

CMMC Level 3: Expert

- **Who it applies to:** Contractors working on the most sensitive DoD programs or critical infrastructure.
- **Requirements:**
  - Fulfill all CMMC Level 2 Requirements
  - Implement 24 additional controls from NIST SP 800-172 to combat advanced persistent threats (APTs).
- **Assessment:**
  - Conducted by the DCMA DIBCAC.
  - Results submitted to eMASS.

KEY TIMELINES AND PHASED ROLLOUTS

Here's a look at the CMMC timeline:

- **December 16, 2024**: CMMC assessments officially transition to being performed by C3PAOs, rather than the DoD's DIBCAC.
- **Late Spring 2025:** Title 48 rule is expected to take effect, enabling CMMC requirements to appear in new federal contracts.

Phased Rollout of CMMC Requirements

Phase 1: Begins with the introduction of CMMC self-assessments in contracts as a condition of award. This phase focuses on CMMC Level 1 (FCI) and Level 2 (CUI) self-assessments.

Phase 2: Starts one year after Phase 1, requiring CMMC Level 2 C3PAO certification as a condition of award.

Phase 3: Begins one year after Phase 2, introducing Level 3 certification as a condition of award, while Level 2 certifications can be added to the option periods of existing contracts.

Phase 4: Launches one year after Phase 3, allowing CMMC requirements to be included in all contracts and option periods, both new and previously awarded.

THE ROLE OF MSPS AND EXTERNAL SERVICE PROVIDERS

Organizations pursuing CMMC compliance can outsource IT services to Managed Service Providers (MSPs) or other External Service Providers (ESPs). Notably:

- MSPs no longer need to hold the same or higher CMMC certification level as their client.
- However, any services the MSP provides will fall "in-scope" for CMMC and must be evaluated during the organization's C3PAO assessments (every 3 years) and annual self-assessments.
- For MSPs supporting multiple CMMC clients, managing compliance requirements can quickly become overwhelming.

Working with CMMC-certified MSPs simplifies the process for both the client and the provider, reducing the complexity of assessments and ensuring smoother compliance.

IMPLICATIONS FOR SUBCONTRACTORS

While CMMC requirements won't begin appearing in contracts until Spring 2025, organizations need to act now to remain competitive.

Prime contractors will likely start assembling teams of certified subcontractors well before CMMC clauses are added to contracts. Subcontractors that delay certification risk being excluded from teaming opportunities, losing market share, and sacrificing their competitive edge—regardless of how qualified they may otherwise be.

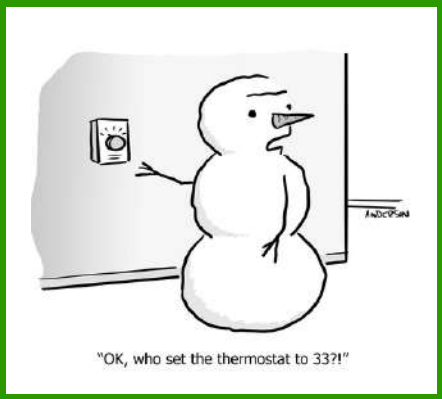
continued on page 4...

BEWARE OF WIFI SQUATTING

When did you last check who has access to your WiFi network? If it's been a while, you'll probably be surprised by who's hanging around. Managing your WiFi access is an important step to keeping your data safe because unwanted WiFi squatters could, at best, slow your WiFi speeds and, at worst, have access to any device or file connected to your network, like household security cameras.

To see who has access to your WiFi, find your router's IP address (you can find instructions online about how to do this), type the IP address into your browser and log in. Next, look for a list called "DHCP Client" or "Connected Devices." Review the list, and if any unknown devices are on it, update your WiFi password and reconnect only the devices you trust.

CARTOON OF THE MONTH



...continued from page 3

of CMMC and the anticipated FAR CUI rule will redefine the landscape for federal contractors. CMMC is well underway, with compliance requirements beginning to appear in DoD contracts in phases starting December 2024.

However, the FAR CUI rule - expected to be finalized as early as the end of 2024 - extends similar requirements to all contractors working with federal agencies, not just the DoD. This means that organizations handling Controlled Unclassified Information (CUI) will need to adhere to NIST SP 800-171 standards regardless of which agency they serve.

For businesses providing goods or services to the U.S. Federal Government, these requirements are non-negotiable. Whether you're navigating the complexities of CMMC or preparing for FAR CUI compliance, it's critical to begin implementing robust cybersecurity measures now. Being proactive will not only ensure compliance but also protect your organization's place in the competitive federal contracting market.

If your organization needs guidance in navigating these regulations, consider leveraging our expertise as your trusted compliance and cybersecurity partners (Compliancy Sherpa & AdRem Systems Corporation). Preparing today will save time, money, and opportunities tomorrow. The path to compliance may be complex, but it is an essential step toward securing sensitive government information in an increasingly vulnerable cyber landscape.

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.

PRESENTED TO YOU BY SHERPA, AN ADREM SYSTEMS COMPANY:

SHERPA An AdRem Company SYSTEMS

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

Welcome & Congratulations
BRIAN MITCHELL

We're excited to welcome our new Systems Support Technician, Brian Mitchell and celebrate his impressive achievements since joining us!

Brian has successfully completed multiple certifications, including Kaseya Certified Technician in K365 End-point and Datto Cybersecurity, and the fundamentals of Remote IT and Security Management.

These accomplishments showcase Brian's dedication to advancing his technical expertise and reflect our team's ongoing commitment to excellence. We're proud to have Brian on board and look forward to the valuable contributions he will bring to our clients. Congratulations, Brian, on your hard work and success!

Passion is the key to success – that's what many of us have been taught to believe. If you want to be great, you must be passionate. However, Tim Grover believes we've been told wrong.

Tim Grover is a renowned speaker, author and performance coach with over 20 years of experience speaking to businesses, entrepreneurs and leadership teams aiming to be the top in their fields. Known for his work with athletes like Michael Jordan, Kobe Bryant and Dwyane Wade, Grover teaches audiences the mindset of elite professionals so they can apply it to their own success. At a recent industry conference, Grover shared his secret to success: It's not passion that equates to success. It's obsession.

Be Obsessed

Grover draws a clear line between being interested in something and being obsessed with it. "Interest is passive," he explains. If you want to take your business to the next level, you must be all in because when you're obsessed, you pay attention to every tiny detail. As a performance coach, Grover read every injury report for his athletes so he knew how to lace their shoes. He watched hours of video footage and knew every step and landing so he could design training plans. "That's obsession," he says. "That's why they kept me around for such a long time."

Act On Your Passions

"You don't follow your passion," Grover explains. "You act on it. You excel at it." In business, hesitation can lead to missed opportunities. Once a decision is made, you must fully commit to it because excellence is a long game. There will be moments of pressure driving you beyond your comfort zone and moments that feel very isolating. "Excellence creates distance. It creates distance between you, your friends, your enemies, your family, your free time," Grover says. This isolation isn't necessarily negative; it's a byproduct of striving for greatness. It will separate you from everyone who is average – from people who don't understand the behind-the-scenes work it takes to truly succeed in your passion. People will try to pull you down, either out of jealousy or a lack of understanding, but excellence requires a singular focus that many won't understand.

Balance Is A Myth

People often say that successful people need balance. Grover argues that if you try to balance everything – work, life, relationships – while striving for success, you'll be mediocre at all of them. You'll never grow if you're pulled in too many directions. The key to success is ditching balance, focusing on fewer, more important priorities and cutting out distractions. "Everyone has time for what they put first," he explains.

Excellence is a long-term journey that demands obsession, action and a refusal to settle for mediocrity. "Write your own story," Grover says. Put down the self-help books and "look deep down inside yourself and stop looking for everybody else to get you to that next level."

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

AdRem SYSTEMS

INSIDE THIS ISSUE

November Answer Key

Safe Cyber Puzzle

ARE YOU MANAGING YOUR VENDOR SECURITY RISKS?

As the year winds down, innovative businesses often reflect on what's gone right – and what needs improvement. Beyond wrapping up projects and planning for next year, one critical task shouldn't be overlooked: managing vendor security risks. Vendors play an essential role in your business's success, but they also present a severe cybersecurity risk if you don't vet and monitor them effectively, especially if they handle sensitive data.

What's A Vendor Risk?

Many businesses rely on trusted vendors, such as cloud services or file-sharing tools, to carry out day-to-day operations. If that vendor gets hacked, your sensitive data is suddenly – and dangerously – exposed. A perfect example is the 2023 MOVEit Transfer breach, where attackers exploited vulnerabilities in the vendor's software, giving them access to critical data like customer information and business records for thousands of organizations. BlueVoyant's State of Supply Chain Defense report showed that organizations experienced, on average, 4.16 supply chain breaches in 2023 that impacted operations.

Vendor breaches are more than annoying – they could also lead to data loss, diminished customer loyalty or even legal issues. This year, consider adding these best practices to your end-of-year review to manage your vendor risk:

1. Review Vendor Contracts
Like you, vendors need to be held accountable for following industry-standard practices like encryption, secure data storage and incident response protocols. Start your vendor risk review by checking to see if your contracts have the necessary security clauses, and make sure your agreements outline these expectations clearly so you and your vendors know what's at stake.

2. Conduct Vendor Security Audits
If you haven't done it recently, it's time for a thorough security audit of your high-risk vendors. This will help you understand if they're implementing strong cybersecurity measures, such as multifactor authentication, encryption and regular system updates. Knowing where your vendors stand gives you a better handle on your own security.

3. Monitor For Emerging Risks
Cyberthreats evolve quickly and so do the risks your vendors face. Regular monitoring of your vendor's security practices, like tracking vulnerabilities or breaches, will keep you on top of any emerging threats.

4. Update Your Vendor List
Now is a good time to clean house. Cut ties with vendors who aren't living up to your security standards and tighten your relationship with those who are proactive about protecting your data. Consider creating standardized onboarding and offboarding processes for vendors, too, so old vendors don't have unwarranted access to your organization.