CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #130

NEWS:

House Passes Bill Requiring Federal Contractors to Implement Vulnerability Disclosure Policies

Original Source:SecurityWeek by Eduard Kovacs

The U.S. House of Representatives has recently passed a bill that mandates federal contractors to establish vulnerability disclosure policies.

This legislative move aims to strengthen the security of federal digital assets by ensuring that vulnerabilities are systematically reported and addressed.

The bill stipulates clear guidelines for contractors on how to manage and respond to reported vulnerabilities effectively.

This initiative underscores the government's commitment to bolstering national cybersecurity infrastructure and fostering a more secure cyber environment for public and private sector collaborations.

CyberSecurity Advisors Network

NEWS:

2. Ethereum private key stealer on PyPI downloaded over 1,000 times

Original Source: BleepingComputer by Bill Toulas

A malicious package designed to steal Ethereum private keys was recently discovered on the Python Package Index (PyPI), downloaded over 1,000 times before its removal.

This deceptive package, masquerading as a legitimate tool, underscores the growing threat in software supply chains where attackers exploit trust to distribute malware.

The incident highlights the critical need for developers and users to exercise heightened vigilance when integrating third-party code, emphasising the importance of verifying sources and maintaining rigorous security protocols to safeguard sensitive cryptocurrency assets.

CyberSecurity Advisors Network

NEWS:

3. Women Faced the Brunt of Cybersecurity Cutbacks in 2024

Original Source: Dark Reading by Kristina Beek

In 2024, the cybersecurity industry witnessed significant cutbacks that disproportionately impacted women, exacerbating existing gender disparities in tech roles.

These reductions not only led to fewer women in cybersecurity positions but also stalled efforts towards achieving diversity and inclusivity within the sector.

The situation calls for urgent implementation of supportive measures and policies aimed at recruiting, retaining, and advancing women in technology, particularly in cybersecurity fields.

Enhancing gender diversity is not just a matter of equity; it enriches problem-solving and strengthens the overall resilience of cybersecurity defences, making it imperative for the industry to address these challenges proactively.

CyberSecurity Advisors Network

NEWS:

4. Malicious Chrome extensions can spoof password managers in new attack

Original Source: BleepingComputer by Bill Toulas

Recent reports have identified a new type of cyber attack involving malicious Chrome extensions that can impersonate legitimate password managers.

These deceptive extensions are capable of stealing login credentials by tricking users into inputting their information, believing they are using their trusted password management tools.

This emerging threat highlights the necessity for users to scrutinise browser extensions carefully before installation and emphasises the importance of sourcing extensions from reputable developers only. It also calls for enhanced security measures by browser and extension marketplaces to prevent such malicious activities.

CyberSecurity Advisors Network

NEWS:

5. BadBox Botnet Powered by 1 Million Android Devices Disrupted

Original Source: Security Week by Ionut Arghire

The BadBox botnet, which harnessed the power of over 1 million compromised Android devices, has recently been disrupted.

This vast network was used for large-scale DDoS attacks and other malicious activities, posing significant threats to online security.

The disruption marks a significant victory for cybersecurity teams, highlighting the effectiveness of coordinated efforts in combating such extensive cyber threats. It also underscores the ongoing need for robust mobile device security measures and public awareness about the risks of downloading unverified applications, which often serve as entry points for malware.

CyberSecurity Advisors Network

NEWS:

6. Over 1,000 WordPress Sites Infected with JavaScript Backdoors Enabling Persistent Attacker Access

Original Source: The Hacker News by Ravie Lakshmanan

More than 1,000 WordPress sites have been compromised with JavaScript backdoors, allowing attackers persistent and covert access.

This widespread issue highlights a significant vulnerability in website security, particularly affecting sites with outdated plugins or weak admin credentials.

The malicious JavaScript enables cybercriminals to manipulate site content, steal data directly from users, and potentially leverage the sites for further attacks.

This situation calls for immediate action from site administrators to update and secure their systems, implement stringent security measures such as regular audits, and educate users on the importance of strong password policies and regular updates to prevent future breaches.

CyberSecurity Advisors Network

NEWS:

7. Ransomware Attacks Build Against Saudi Construction Firm

Original Source: Dark Reading Global by Robert Lemos

A Saudi construction firm is currently under siege from a series of escalating ransomware attacks, highlighting a significant vulnerability within the infrastructure sector.

These attacks not only threaten the operational continuity and data integrity of the firm but also expose potential security lapses in industry-wide cybersecurity practices.

The situation underscores the critical need for robust cybersecurity measures, including regular system updates, comprehensive employee training, and advanced threat detection mechanisms. It also calls for a collaborative approach to cybersecurity, with increased sharing of threat intelligence and best practices within the sector to mitigate future risks.

CyberSecurity Advisors Network

NEWS:

8. Espionage Actor 'Lotus Blossom' Targets Southeast Asia

Original Source: Dark Reading by Alexander Culafi

The espionage group known as 'Lotus Blossom' continues to intensify its cyber espionage efforts across Southeast Asia.

Leveraging sophisticated tactics, the group targets government and military sectors to gather sensitive information that could influence regional security dynamics.

This persistent threat underscores the critical need for heightened cybersecurity measures within these sectors.

Enhanced vigilance, advanced threat detection systems, and continuous cybersecurity training are imperative to defend against such state-sponsored activities and to safeguard national security interests in the region.

CyberSecurity Advisors Network

NEWS:

9. SandboxAQ Joins UN AI Hub to Bolster Cybersecurity and Drive AI Innovation

Original Source: IT Security Guru

SandboxAQ has partnered with the UN AI Hub to enhance global cybersecurity measures and foster innovation in artificial intelligence.

This collaboration aims to leverage SandboxAQ's expertise in quantum computing and AI to develop solutions that address critical security challenges faced by nations worldwide.

By integrating advanced AI technologies, the partnership seeks to create more resilient cybersecurity infrastructures and drive technological advancements that benefit global security and governance.

This initiative not only highlights the potential of AI in enhancing cybersecurity but also emphasises the importance of international cooperation in tackling complex digital threats.

CyberSecurity Advisors Network

NEWS:

10. US indicts 12 Chinese nationals for vast espionage attack spree

Original Source: Cyberscoop by Matt Kapko

The United States has indicted 12 Chinese nationals in connection with a comprehensive espionage operation targeting sensitive U.S. industrial and technological sectors.

This sweeping indictment underscores the ongoing geopolitical tensions and the extensive nature of state-sponsored cyber espionage activities.

The accused are alleged to have conducted sophisticated cyber operations to steal trade secrets and critical data, compromising national security and the competitive edge of U.S. businesses.

The case highlights the critical need for robust cyber defenses and international collaboration to combat these high-stakes threats.

CyberSecurity Advisors Network

NEWS:

11. Open-source tool 'Rayhunter' helps users detect Stingray attacks

Original Source: BleepingComputer by Bill Toulas

Rayhunter, an innovative open-source tool, has been developed to empower individuals and organisations to detect Stingray attacks—covert surveillance methods that intercept mobile phone communications.

This tool is particularly crucial in protecting privacy rights as it enables users to identify and mitigate unauthorised cell tower simulators used for eavesdropping.

Rayhunter's availability underscores the importance of community-driven solutions in enhancing digital privacy and security. It represents a significant step forward in the fight against intrusive surveillance technologies, offering a proactive approach to safeguard personal communications.

CyberSecurity Advisors Network

NEWS:

12. Major ransomware attack sees Tata Technologies hit - 1.4TB dataset with over 730,000 files allegedly stolen

Original Source: Tech Radar by Ellen Jennings-Trace

Tata Technologies has been severely impacted by a major ransomware attack, resulting in the theft of approximately 1.4 terabytes of data, encompassing over 730,000 files.

This significant security breach underscores the escalating threat landscape that corporations worldwide are facing.

The attack not only highlights the need for stringent cybersecurity measures but also puts a spotlight on the vulnerabilities that can be exploited in critical business infrastructures.

The incident calls for an urgent review and reinforcement of digital defenses to prevent future occurrences and protect sensitive corporate information.

CyberSecurity Advisors Network

NEWS:

13. VMware Security Flaws Exploited in the Wild—Broadcom Releases Urgent Patches

Original Source: The Hackers News by Ravie Lakshmanan

Recent discoveries have revealed significant security vulnerabilities in VMware products, which have been actively exploited in the wild.

These flaws could allow attackers to execute code remotely and escape from secured environments, posing severe risks to enterprises relying on VMware for their virtual infrastructure.

In response, Broadcom has swiftly released urgent patches to address these vulnerabilities. Organizations are urged to apply these security updates immediately to protect their systems from potential breaches and maintain the integrity of their operational environments.

This incident highlights the ongoing need for vigilance and prompt action in the face of emerging cybersecurity threats.

CyberSecurity Advisors Network

NEWS:

14. Threat Actor 'JavaGhost' Targets AWS Environments in Phishing Scheme

Original Source: Dark Reading by Alexander Culafi

The 'JavaGhost' threat actor is currently targeting AWS environments through a sophisticated phishing scheme designed to compromise enterprise cloud infrastructures.

By exploiting vulnerabilities in AWS configurations, JavaGhost has been able to execute phishing attacks that deceive users into revealing their credentials.

This campaign underscores the importance of stringent cloud security practices, including regular audits and employee training to recognise phishing attempts.

Organisations using AWS must enhance their vigilance and deploy multi-layered security measures to prevent such breaches and protect their critical cloud assets.

CyberSecurity Advisors Network

CYAN APAC EVENT IN SYDNEY!

Mark your calendars—this is one event you won't want to miss!

In a world where cyber threats are reshaping global power dynamics, understanding their geopolitical implications has never been more critical. This event will provide unique insights into how the evolving cyber landscape impacts nations, organisations, and individuals, offering strategies to navigate these challenges with clarity and resilience.

We'll begin with a keynote from acclaimed cybersecurity advisor Dan Elliott, followed by a panel discussion moderated by Dr. Saba Bagheri, Cyber Threat Intelligence Manager at BUPA, featuring

- **Peter Evans, CISO at NSW Police Force**
- **Robbie Abraham, Head of Cyber Threat Intelligence at Newfold Digital**

NEWS:

15. Congress eyes bigger cyber role for NTIA amid telecom attacks

Original Source: Cyberscoop by Matt Bracken

In response to increasing cyber attacks targeting the telecommunications sector, Congress is considering legislation to expand the cyber responsibilities of the National Telecommunications and Information Administration (NTIA).

This move aims to bolster the United States' defences against sophisticated cyber threats that disrupt essential communication services.

By enhancing the NTIA’s capabilities, lawmakers hope to improve coordination across federal agencies and strengthen the resilience of critical infrastructure.

The proposed changes underscore the urgency of adapting governmental cyber strategies to meet the evolving landscape of digital threats.

CyberSecurity Advisors Network

NEWS:

16. Cisco warns of Webex for BroadWorks flaw exposing credentials

Original Source: BleepingComputer by Sergiu Gatlan

Cisco has issued a warning about a critical flaw in Webex for BroadWorks that could expose user credentials, posing a significant security risk.

This vulnerability allows unauthorised access to sensitive information, potentially enabling attackers to intercept and manipulate communications. Cisco has recommended immediate updates and has provided patches to mitigate this vulnerability.

This incident highlights the continuous need for vigilance and prompt software updates in safeguarding communication tools from emerging cyber threats.

Organizations are urged to apply these patches without delay to protect their data and maintain the integrity of their communication channels.

CyberSecurity Advisors Network

NEWS:

17. Microsoft Teams tactics, malware connect Black Basta, Cactus ransomware

Original Source: BleepingComputer by Lawrence Abrams

Recent analysis has revealed that cybercriminals employing Black Basta and Cactus ransomware are leveraging Microsoft Teams as a vector for their attacks.

These groups use malicious tactics, such as embedding malware within seemingly legitimate communications, to exploit the popular collaboration platform.

The use of Microsoft Teams enables these attackers to bypass traditional security measures and gain unauthorised access to corporate networks.

This development calls for organizations to enhance their security protocols concerning communication tools and educate employees about the risks of malware in everyday applications, ensuring robust defenses against these sophisticated cyber threats.

CyberSecurity Advisors Network

NEWS:

18. New polyglot malware hits aviation, satellite communication firms

Original Source: BleepingComputer by Bill Toulas

A sophisticated new form of polyglot malware has been identified targeting aviation and satellite communication firms, posing significant security challenges.

This malware uniquely blends multiple functionalities, allowing it to act both as a data stealer and a disruptor of communication systems.

The attacks highlight vulnerabilities within critical infrastructure sectors and underscore the urgent need for enhanced cybersecurity measures.

Firms in these industries are advised to conduct thorough security audits, update their systems regularly, and train staff to recognise signs of malicious activities to safeguard against such advanced threats.

CyberSecurity Advisors Network

NEWS:

19. 3 VMware Zero-Day Bugs Allow Sandbox Escape

Original Source: Dark Reading by Jai Vijayan

Three critical zero-day vulnerabilities have been discovered in VMware software, allowing attackers to escape from virtualised environments and execute code on the host machine.

These vulnerabilities pose severe risks to enterprises relying on VMware for virtualisation, as they could lead to full system compromise if exploited.

VMware has responded by releasing urgent patches to address these security flaws. Organizations are strongly advised to apply these updates immediately to protect their systems from potential attacks.

This incident highlights the ongoing need for proactive security practices and rapid response to emerging threats in virtualisation technology.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

20. Hunters International ransomware claims attack on Tata Technologies

Original Source: BleepingComputer by Bill Toulas

Tata Technologies recently fell victim to a significant ransomware attack by Hunters International, resulting in the theft of over 1.4 terabytes of sensitive data, including more than 730,000 files.

This breach underscores the growing threat of ransomware attacks targeting major corporations, highlighting the potential for substantial operational disruption and financial loss.

In response to the attack, Tata Technologies is taking robust measures to bolster their cybersecurity defences and mitigate the impact of the breach.

This incident serves as a critical reminder for all companies to enhance their data protection strategies and prepare for the possibility of similar cyber threats.

CyberSecurity Advisors Network

NEWS:

21. More than 86K IoT devices compromised by fast-growing Eleven11

Original Source: Cybersecurity Dive by David Jones

The Eleven11 botnet, a rapidly expanding network, has compromised over 86,000 IoT devices worldwide, demonstrating the increasing vulnerabilities in connected technology.

This botnet exploits weak default passwords and unpatched security flaws to control devices, using them for large-scale DDoS attacks and other malicious activities.

The widespread impact underscores the critical importance of securing IoT devices with strong, unique passwords and regular firmware updates. It highlights the necessity for manufacturers and users to implement more rigorous security measures to prevent such infiltrations and protect the integrity of IoT ecosystems.

CyberSecurity Advisors Network

NEWS:

22. Polish Space Agency Hit by Cyberattack

Original Source: Security Week by Ionut Arghire

The Polish Space Agency recently experienced a significant cyberattack, highlighting vulnerabilities in national security and space exploration sectors.

This breach compromised sensitive data, potentially affecting critical operations and international collaborations.

The incident emphasises the urgent need for enhanced cybersecurity protocols and systems within agencies involved in space technology and research. It also calls for increased cooperation among international partners to bolster defenses against such sophisticated threats, ensuring the protection of vital infrastructure and information in the expanding arena of space exploration.

CyberSecurity Advisors Network

NEWS:

23. Big tech opposes YouTube exemption from Australia's social media ban

Original Source: itNews by Renju Jose

Major technology companies are challenging an exemption that would allow YouTube to operate under Australia's proposed social media ban, citing concerns over fairness and regulatory consistency.

The ban, aimed at protecting users from harmful online content, has sparked debate among tech giants, who argue that all platforms should be held to the same standards.

This opposition highlights the complexities of regulating digital platforms while ensuring competitive equity. It underscores the need for clear, equitable regulations that balance user safety with fair market practices, crucial for maintaining a healthy digital ecosystem.

CyberSecurity Advisors Network

ANALYSIS:

24. Cybersecurity's Future Is All About Governance, Not More Tools

Original Source: Dark Reading by Shirley Salzman

Shirley Salzman, writing for Dark Reading, argues that the future of cybersecurity isn’t about hoarding tools but about mastering governance.

While technology plays a role, true resilience comes from strong policies, risk management, and compliance frameworks that align security strategies with business objectives.

Salzman emphasises that prioritising governance over endless tool acquisition strengthens operational resilience, mitigates risks proactively, and ensures organizations can adapt to evolving threats.

By embedding governance into cybersecurity, businesses create a security posture that’s not just reactive but strategic, scalable, and built for long-term digital defence.

CyberSecurity Advisors Network

ANALYSIS:

25. Identity: The New Cybersecurity Battleground

Original Source: The Hacker News

The Hacker News staff highlights identity as the new battleground in cybersecurity, with attackers shifting from exploiting system vulnerabilities to targeting user credentials.

Protecting digital identities now requires more than just passwords—it demands multi-factor authentication, continuous monitoring, and behavioural analytics to detect and block unauthorised access.

As identity theft and credential-based attacks grow more sophisticated, organizations must prioritize advanced identity protection measures to safeguard individuals and digital infrastructure from evolving cyber threats.

CyberSecurity Advisors Network

ANALYSIS:

26. Enterprise AI Through a Data Security Lens: Balancing Productivity With Safety

Original Source: Dark Reading buy Adam Strange

Writing for Dark Reading, Adam Strange emphasises that as AI continues reshaping business operations, balancing productivity with stringent data security is critical.

Organisations must embed security-first principles into AI deployments, ensuring sensitive information is protected from misuse or breaches.

Strong data governance, encryption, and access controls are essential to maintaining trust in AI-driven environments. Strange argues that without prioritising security alongside innovation, businesses risk compromising both regulatory compliance and long-term growth in an AI-powered corporate landscape.

CyberSecurity Advisors Network

ANALYSIS:

27. Tech companies’ proposed new safety codes won’t protect all kids online

Original Source: InnovationAus by Toby Murray

Toby Murray of InnovationAus critiques tech companies’ proposed safety codes, arguing they fail to offer comprehensive protection for all children online.

While these measures represent progress, they still leave critical gaps, particularly for vulnerable users who need the most protection.

Murray calls for stronger regulatory enforcement, ensuring platforms take real accountability rather than relying on voluntary commitments.

Without broader, legally binding safeguards, children remain at risk, highlighting the urgent need for policies that prioritize child safety over corporate interests.

CyberSecurity Advisors Network

ANALYSIS:

28. Cyberwarfare, Elections, and the Role of Encryption in Protecting Democracy

Original Source: PrivID (Substack)

PrivID (Substack) highlights encryption as a crucial safeguard for democracy, especially as cyberwarfare threats escalate.

Strong encryption protects voter data and election integrity from manipulation, ensuring that democratic outcomes remain free from interference. Weakening these protections risks exposing electoral systems to hostile actors, eroding public trust.

The analysis calls on governments to uphold robust encryption standards, reinforcing digital voting security, transparency, and resilience against cyber threats that seek to undermine democratic processes at a time when trust in institutions is already fragile.

CyberSecurity Advisors Network

ANALYSIS:

29. Why Cybersecurity Jobs Are Hard to Find Amid a Worker Shortage

Original Source: Dark Reading by Andrey Leskin

Andrey Leskin of Dark Reading examines the paradox of a cybersecurity job market plagued by both a talent shortage and hiring difficulties.

Despite high demand, many skilled candidates struggle to secure roles due to rigid job descriptions, unrealistic experience requirements, and a preference for niche expertise over adaptable skills. Instead of fostering talent, companies are narrowing the pool by demanding certifications over potential. The analysis calls for a shift in hiring strategies—investing in internal development, easing entry barriers, and creating pathways for emerging professionals to bridge the cybersecurity skills gap before it widens further.

CyberSecurity Advisors Network

ANALYSIS:

30. Exploiting DeepSeek-R1: Breaking Down Chain of Thought Security

Original Source: Trend Micro by Trent Holmes & Willem Gooderham

Trent Holmes and Willem Gooderham of Trend Micro uncover critical security flaws in DeepSeek-R1, exposing weaknesses in its chain-of-thought reasoning that attackers can exploit.

These vulnerabilities enable adversaries to manipulate AI outputs, leading to misinformation, biased responses, or data leaks.

The findings highlight the urgent need for security-first AI development, where transparency, rigorous testing, and adversarial resilience are prioritised.

Without stronger safeguards, large language models remain susceptible to manipulation, posing risks to trust, decision-making, and the ethical use of AI-driven systems.

CyberSecurity Advisors Network

CyAN Members-Only Quiz Challenge

Are You In the #CyANQuiz?

Hey CyAN Champions,

Ready to test your cybersecurity know-how? Join our Quarterly #CyANQuiz Challenge, starting this month!

Each quiz offers a chance to **climb higher on the leaderboard**, with points accumulating throughout the year.

🔥 **Engaging Challenges:** Tackle tough cybersecurity questions and sharpen your expertise.

🏆 **Compete for Glory:** Match wits with fellow CyAN pros quarterly and vie for awesome prizes and exclusive CyAN perks!

📅 **Mark Your Calendar:** Kick off is March 31st!

Compete throughout the year with each quiz adding to your total score. **Top year-end champions win big rewards (free membership for a year anyone!)!**

Join the fun—this isn't just a quiz, it's a year-long challenge to **shine in the CyAN community**.

Are you ready? **Check your email for further details!**

CyAN Cybersecurity Advisors Network

STATISTICS & INSIGHTS powered by evisec

31. Highlights from this week's cybersecurity research by evisec - CRD #18

Original Source: CyAN Member and evisec CEO Henry Röigas

- Ransomware payments prioritize speed over restoration: 96% of cases involve data exfiltration, but only 30% result in payments—mainly to prevent leaks or accelerate recovery, not restore systems.
- Security careers: high pay, low retention: Over 60% of professionals consider leaving due to stagnation. Security architects earn up to $206K, but return-to-office mandates risk talent loss.
- Hybrid work & BYOD risks: 98% of organizations report BYOD violations, with 90% allowing personal device access to corporate data, exposing security gaps.
- Global threats surge: China-linked activity is up 150%, vishing skyrockets 442%, malware-free attacks hit 79%, and breakout times drop to 48 minutes, demanding faster response.
- Software security paradox: OWASP pass rates double, but security debt worsens—fix times have increased fivefold in 15 years despite improved critical risk mitigation.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

32. CyAN's Position on Encryption Backdoor Legislation

Original Source: CyAN Blog by CyAN Staff

CyAN firmly opposes encryption backdoors, warning that such policies undermine global cybersecurity. While governments argue they are necessary for law enforcement, the reality is they create systemic vulnerabilities that can be exploited by cybercriminals and hostile nation-states.

Weakening encryption doesn't just affect criminals—it puts businesses, critical infrastructure, and everyday users at risk.

Instead of compromising security, CyAN advocates for stronger encryption policies that protect privacy, safeguard data integrity, and ensure a more resilient digital landscape without handing malicious actors an easy entry point.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

33. Phishing, Smishing, and Quishing—How Many Ways Can We Get Scammed?

Original Source: by CyAN General Secretary Fel Gayanilo

CyAN Gen Sec Fel Gayanilo dives into the ever-expanding world of digital scams, where cybercriminals exploit email (phishing), SMS (smishing), and QR codes (quishing) to trick users into handing over sensitive data. As fraud tactics evolve, so must our defences.

Many scams rely on urgency and deception, preying on human instincts rather than technical vulnerabilities.

Fel emphasises the importance of skepticism, user awareness, and layered security to mitigate these threats.

The best defence? Think before you click—because in today's cyber landscape, convenience often comes with a hidden cost.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

34. Dynamic Resilience: A Framework for Synergizing Operational Agility and Economic Security in the Era of Digital Transformation

By CyAN Staff

CyAN explores Dynamic Resilience, a strategy that merges cybersecurity, business agility, and economic security to help organizations navigate digital transformation without increasing risk.

As cyber threats evolve, businesses must move beyond static defences and embrace flexible security frameworks that adapt in real time.

The key lies in balancing innovation with proactive risk management, ensuring security measures scale with technological advancements.

By integrating security into operational agility, organisations can sustain growth, safeguard assets, and maintain resilience in an unpredictable digital landscape.

CyberSecurity Advisors Network

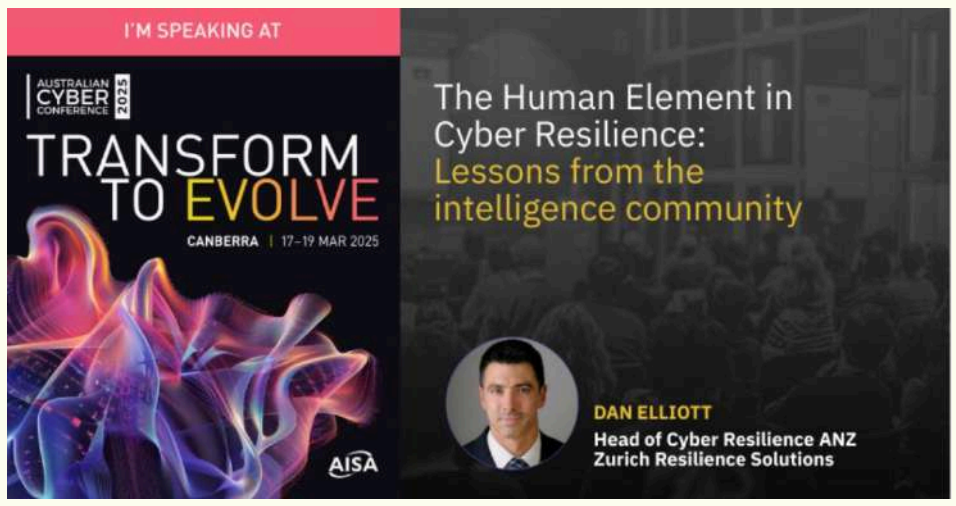
CyAN Member's News:

We at CyAN are ALWAYS overjoyed to celebrate our members successes and their contributions to the cybersecurity community!

We're immensely proud to share that Dan Elliott, a highly valued member of our CyAN community, and internationally acclaimed cybersecurity advisor is a finalist in the prestigious 2025 Australian Cyber Awards in the Cybersecurity Professional of the Year in Professional and Financial Services category!

His nomination is a testament to his dedication to the field of cybersecurity, his commitment to collaboration with his clients and peers and his dedication to sharing his extensive experience and expertise across the sector.

Join us in celebrating his well-deserved recognition!



On March 18th Dan is also speaking at the Australian Information Security Association (AISA) on the topic of The Human Element in Cyber Resilience: Lessons from the intelligence community. If you're in Canberra, you won't want to miss this!

UPCOMING CyAN and CyAN Partner EVENTS:

- **CyAN APAC: The Geopolitical Impacts of Cyber Threats: From Espionage to Influence keynote by Dan Elliot, March 12, Peoplebank, Sydney (save the date, more info on page 10 of this newsletter!)**
- **Trust & Safety Forum at Forum INCYBER Europe (FIC), Lille, France: April 1-2**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April**
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April**
- **GISEC: Dubai Word Trade Center, Dubai, UAE: 6- 8 May**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK**
- **World AI Technology Expo UAE, Dubai, UAE: 14-15 May 2025 https://worldaiexpo.i**
- **MaTeCC, Rabat, Morocco: 7-9 June, 2025**

CyAN Cybersecurity Advisors Network

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!
#SharingIsCaring