CyAN

Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #134

CyAN Cybersecurity Advisors Network

NEWS:

Judge blocks Elon Musk’s Doge from accessing social security records

Original Source: The Guardian by Guardian Staff & Agencies

A federal judge has issued a restraining order preventing Elon Musk’s Department of Government Efficiency (Doge) from accessing Social Security Administration (SSA) records, citing privacy concerns and potential data misuse.

The lawsuit, filed by advocacy groups, argues that Doge’s demand for non-anonymised data amounts to a fishing expedition, with risks of exposing sensitive personal information.

Musk, appointed to cut government spending, has faced criticism for aggressive cost-cutting and mass layoffs, fuelling concerns over transparency, oversight, and the ethical handling of federal data.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

2. Ukraine Defense Sector Under Attack Via Dark Crystal RAT

Original Source: Dark Reading by Kristina Beek

Ukraine’s defense sector is facing a new wave of cyberattacks deploying Dark Crystal RAT (DCRat), a powerful malware capable of remote access, data theft, and system manipulation.

Threat actors are using phishing emails and malicious attachments to infiltrate defence networks, raising concerns over national security and battlefield intelligence leaks.

This campaign underscores the increasing cyberwarfare threats targeting Ukraine’s military infrastructure, reinforcing the need for enhanced endpoint security, strict access controls, and real-time threat intelligence to mitigate state-sponsored attacks.

Cybersecurity Advisors Network

CyAN

NEWS:

3. RansomHub ransomware uses new Betruger 'multi-function' backdoor

Original Source: BleepingComputer by Sergiu Gatlan

The RansomHub ransomware group has integrated Betruger, a newly discovered multi-function backdoor, to enhance stealth, persistence, and payload deployment.

Betruger allows attackers to bypass security defences, exfiltrate sensitive data, and execute ransomware operations with greater efficiency.

This evolution in ransomware tactics highlights the growing sophistication of double-extortion techniques, where attackers encrypt data while also threatening public leaks.

Organisations must prioritise endpoint security, network segmentation, and real-time monitoring to defend against these advanced ransomware threats.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

4. HellCat hackers go on a worldwide Jira hacking spree

Original Source: BleepingComputer by Ionut Ilascu

The HellCat hacking group is actively targeting Jira servers worldwide, exploiting unpatched vulnerabilities to gain unauthorised access, steal sensitive data, and deploy malware.

The attacks focus on exfiltrating corporate and government project management data, posing a severe risk to intellectual property and internal communications.

Security researchers warn that many organisations have failed to apply critical updates, leaving them vulnerable.

Experts recommend immediate patching, strong access controls, and continuous monitoring to prevent these intrusions and protect sensitive project data.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

5. Nation-state groups hit hundreds of organizations with Microsoft Windows zero-day

Original Source: Cyberscoop by Matt Kapko

Nation-state hacking groups are actively exploiting a Microsoft Windows zero-day vulnerability, compromising hundreds of organisations across critical sectors. The flaw allows attackers to escalate privileges, gain persistent access, and deploy malware, making it a valuable tool for espionage and disruptive cyber operations.

Security experts warn that affected organisations must apply available mitigations, enhance endpoint detection, and monitor for unusual activity to prevent exploitation.

This campaign highlights the urgency of timely patching and proactive defence strategies against state-sponsored cyber threats.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

6. India Is Top Global Target for Hacktivists, Regional APTs

Original Source: Dark Reading by Robert Lemos

India has become the top global target for hacktivists and regional APT groups, facing a surge in cyberattacks on critical infrastructure, financial institutions, and government networks.

Motivations range from political activism to state-sponsored espionage, with attackers leveraging sophisticated malware, phishing campaigns, and zero-day exploits.

The rise in threats highlights the urgent need for enhanced cyber defenses, cross-border intelligence sharing, and proactive threat-hunting to mitigate risks against India's expanding digital economy and national security infrastructure.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

7. WhatsApp patched zero-click flaw exploited in Paragon spyware attacks

Original Source: BleepingComputer by Sergiu Gatlan

A critical zero-click vulnerability in WhatsApp was exploited in targeted spyware attacks linked to Paragon, a surveillance firm known for supplying spyware to governments.

The flaw allowed attackers to infect devices without user interaction, exposing victims to surveillance and data theft.

WhatsApp has since patched the issue, but the incident underscores growing concerns over commercial spyware abuse and the need for stronger security measures to prevent sophisticated exploits that threaten privacy and national security.

Users are urged to keep apps updated to protect against emerging threats.

CyberSecurity Advisors Network

8. New Arcane infostealer infects YouTube, Discord users via game cheats

Original Source: BleepingComputer by Bill Toulas

Cybercriminals are spreading the Arcane infostealer via fake game cheats on YouTube and Discord, tricking users into downloading malware disguised as gaming tools.

Once installed, Arcane steals login credentials, financial data, and personal information, posing serious risks to victims. The malware's distribution method leverages the trust gamers place in community-shared content, making detection difficult.

This campaign highlights the dangers of downloading unverified software and the need for stronger user awareness, platform moderation, and security controls to combat evolving infostealer threats.

CyAN Cybersecurity Advisors Network

NEWS:

9. Leaked Black Basta Chats Suggest Russian Officials Aided Leader's Escape from Armenia

Original Source: The Hacker News by Ravie Lakshmanan

Leaked internal chats from Black Basta, a notorious ransomware group, suggest that Russian officials may have helped its leader evade capture in Armenia.

The messages indicate high-level connections that allowed for safe passage out of the country, raising concerns about state-backed cybercriminal protection.

If true, this reinforces fears that Russia is sheltering ransomware operators, complicating international efforts to combat cybercrime.

The revelations highlight the urgent need for stronger global cooperation, sanctions, and law enforcement actions against cybercriminal networks operating with impunity.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

10. Six additional countries identified as suspected Paragon spyware customers

Original Source: Cyberscoop by Tim Starks

Investigations have linked six more countries to the use of Paragon spyware, a powerful surveillance tool marketed for law enforcement but often abused for political espionage.

While Paragon claims it restricts sales to trusted governments, reports suggest its spyware has been used to monitor dissidents, journalists, and activists.

This growing list of suspected customers fuels concerns over the unchecked proliferation of commercial spyware, the lack of international regulations, and the ongoing threats to privacy, press freedom, and human rights in authoritarian-leaning states.

CyberSecurity Advisors Network

CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Have you got what it takes to outsmart your fellow cybersecurity pros? It's time to put your skills to the test in our Quarterly #CyANQuiz Challenge, kicking off on March 31st!

🔹 30 Questions. Timed. No second chances.
🔹 Based on Recent Cybersecurity News & Events – Watch out for recent news and Cybersecurity events.

📅 **Check your email on March 31st for the quiz link**; just click, answer, and climb the leaderboard!
💡 Why Play? Compete, have fun, and win awesome prizes (while proving your cybersecurity dominance!

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

Think you can take the cyber crown? Prove it!

Cybersecurity Advisors Network

CyAN

NEWS:

11. Activist alerts ICC to spyware attack while sharing Libya torture victims' details

Original Source: The Guardian by Stephanie Kirchgaessner & Angela Giuffrida

A human rights activist reported being targeted by spyware while submitting evidence of Libyan torture victims to the International Criminal Court (ICC), raising alarm over the use of surveillance tools to obstruct justice.

The attack, suspected to be politically motivated, highlights the weaponisation of spyware against activists, journalists, and legal professionals.

This incident underscores the urgent need for stricter regulations on commercial spyware, international accountability for misuse, and stronger security measures to protect those working on human rights investigations from digital surveillance and intimidation.

CyberSecurity Advisors Network

NEWS:

12. Ukrainian military targeted in new Signal spear-phishing attacks

Original Source: BleepingComputer by Bill Toulas

A new spear-phishing campaign is targeting the Ukrainian military, using Signal messages to trick personnel into downloading malware.

Attackers impersonate trusted sources, sending malicious links that, once opened, grant unauthorised access to sensitive data and communications.

This tactic marks an evolution in cyber warfare, exploiting encrypted messaging platforms to bypass traditional security measures.

The attack underscores the growing threat of nation-state cyber operations, highlighting the need for enhanced training, stronger authentication protocols, and continuous threat monitoring in military communications.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

13. ClearFake Infects 9,300 Sites, Uses Fake reCAPTCHA and Turnstile to Spread Info-Stealers

Original Source: The Hacker News by Ravie Lakshmanan

A large-scale ClearFake campaign has infected 9,300 websites, using fake reCAPTCHA and Turnstile prompts to trick users into downloading info-stealing malware.

These fraudulent verification screens appear legitimate but deliver malicious payloads that harvest credentials, financial data, and browser-stored information.

The attack highlights the growing sophistication of social engineering tactics, reinforcing the need for stronger website security, user awareness, and advanced threat detection to combat malware campaigns that exploit trust in widely used authentication systems.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

14. Scareware Combined With Phishing in Attacks Targeting macOS Users

Original Source: SecurityWeek by Ionut Arghire

Cybercriminals are combining scareware and phishing tactics to target macOS users, using fake security alerts to trick victims into installing malware or revealing credentials.

These attacks rely on social engineering, displaying fraudulent pop-ups that claim the system is infected, leading users to click malicious links or download rogue software.

The campaign highlights the growing sophistication of macOS-targeted threats, emphasising the need for user awareness, strong endpoint protection, and cautious interaction with unexpected security warnings to prevent falling victim to these scams.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

15. Hackers Exploit Severe PHP Flaw to Deploy Quasar RAT and XMRig Miners

Original Source: The Hacker News by Ravie Lakshmanan

A critical PHP vulnerability is being actively exploited to deploy Quasar RAT and XMRig cryptocurrency miners, allowing attackers to take control of infected systems.

The flaw enables remote code execution, giving hackers a backdoor to steal data, spy on users, and hijack computing resources for cryptomining.

The attack highlights the ongoing risks of unpatched software and the need for immediate updates, stronger access controls, and continuous monitoring to prevent cybercriminals from leveraging PHP-based exploits for espionage and financial gain.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

16. Cybersecurity Experts Are Sounding the Alarm on DOGE

Original Source: TIME by Andrew R. Chow

Security experts are raising concerns over DOGE’s expanding role in financial transactions, warning that its lack of regulatory oversight and growing use in illicit activities make it a prime target for cybercriminals.

The cryptocurrency’s popularity has surged, but its decentralised nature and weak security measures expose users to scams, fraud, and laundering operations.

Experts emphasise the urgent need for stricter compliance frameworks, enhanced monitoring tools, and user education to prevent DOGE from becoming a haven for cybercrime while ensuring financial security in the evolving crypto landscape.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

17. Rules File Backdoor: AI Code Editors Exploited For Silent Supply Chain Attacks

Original Source: Security Affairs by Pierluigi Paganini

Attackers are exploiting AI-powered code editors to inject stealthy backdoors into software supply chains, leveraging manipulated rules files to introduce malicious code without detection.

These silent intrusions bypass traditional security tools, allowing attackers to compromise development environments, steal credentials, and inject vulnerabilities into widely used software.

The rise of AI-assisted coding highlights the urgent need for strict code validation, continuous monitoring, and enhanced security in software development pipelines to prevent exploitation and ensure supply chain integrity.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

18. Critical Fortinet Vulnerability Draws Fresh Attention

Original Source: Dark Reading by Jai Vijayan

A critical vulnerability in Fortinet products is drawing renewed concern as attackers increasingly exploit it to gain unauthorised access to corporate networks.

This flaw allows remote code execution, enabling cybercriminals to steal data, deploy malware, and move laterally within compromised environments.

Security experts warn that many organisations have yet to patch affected systems, leaving them vulnerable to exploitation.

This incident reinforces the urgent need for timely patching, robust access controls, and continuous monitoring to prevent cybercriminals from leveraging known security gaps for large-scale intrusions.

CyAN Cybersecurity Advisors Network

NEWS:

19. California Cryobank, the Largest US Sperm Bank, Disclosed a Data Breach

Original Source: Security Affairs by Pierluigi Paganini

California Cryobank, the largest sperm bank in the U.S., has disclosed a data breach, exposing sensitive client and donor information.

The breach raises concerns over privacy, medical data security, and potential identity theft, as fertility clinics and healthcare-related organisations become increasingly targeted by cybercriminals.

While the full scope of the breach is still under investigation, the incident underscores the need for stronger data protection in the healthcare sector, emphasising encryption, access controls, and stricter cybersecurity measures to safeguard personal medical records from exploitation.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

20. AI Cloud Adoption Is Rife With Cyber Mistakes

Original Source: Dark Reading by Elizabeth Montalbano

Organisations rushing to adopt AI-powered cloud services are making critical security missteps, exposing sensitive data to cyber threats.

Poor access controls, misconfigured APIs, and a lack of encryption have left AI cloud environments vulnerable to breaches and unauthorised access.

Security experts warn that over-reliance on automation without robust governance, compliance, and risk assessment increases exposure to cyberattacks.

To mitigate these risks, companies must implement strict data protection policies, continuous monitoring, and AI-specific security frameworks to safeguard their cloud-based AI operations.

CyberSecurity Advisors Network

Has Trust in Democracy Survived the 2024 Election Year?

The Trust and Safety Forum is hosting a must-attend discussion on elections, disinformation, and democracy’s resilience in the digital age as part of InCyber Forum Europe 2025.

📅 **April 1, 2025 | 🕒 13:45 – 14:30 CET**
📍 **Lille, France | INCYBER FORUM EUROPE 2025**

The Panel:
🎙 **Lorena Martinez** – Head of Editorial Operations, Europe & UK, Logically Facts
🎙 **Laetitia Avia** – Digital Policy Expert, Lawyer & Former French MP
🎙 **Stéphanie Ladel** – OSINT, IMINT & GEOINT Researcher & Trainer
🗣 **Moderated by John Sullivan**, CyAN Board Member & Communications Chief

Discussion Topics:
✅ **Debunking disinformation** – What’s working, and what needs to change?
✅ **The role of fact-checkers** – Minimising misinformation in real time
✅ **Building a balanced political environment** – The resources needed for election integrity

🎟 **Scan the QR code above to get your free visitor’s badge!**

CyAN Cybersecurity Advisors Network

NEWS:

21. UK cybersecurity agency warns over risk of quantum hackers

Original Source: The Guardian by Dan Milmo

The UK's cybersecurity agency has issued a warning about the growing threat of quantum-enabled cyberattacks, urging organisations to prepare for the future impact of post-quantum cryptography.

As quantum computing advances, existing encryption standards risk becoming obsolete, allowing attackers to decrypt sensitive data at unprecedented speeds.

The agency stresses the need for early adoption of quantum-resistant encryption, proactive risk assessments, and collaboration between governments and industry leaders to ensure digital security remains resilient in the face of emerging quantum threats.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

22. Europol warns of AI-driven crime threats

Original Source: itNews

Europol has raised concerns about the increasing use of AI in cybercrime, warning that criminals are leveraging AI-powered tools for more sophisticated phishing, fraud, and deepfake-based scams.

The agency highlights that AI is being used to automate attacks, create highly convincing fake identities, and bypass traditional security measures, making cyber threats harder to detect.

Europol urges governments, businesses, and law enforcement to develop AI-resistant security measures, enhance digital forensics, and adopt stricter regulations to prevent AI from becoming a tool for large-scale cybercrime.

CyberSecurity Advisors Network

23. Hundreds of ‘malicious’ Google Play-hosted apps bypassed Android 13 Security ‘with ease’

Original Source: itNews / Bitdefender

Security researchers have uncovered hundreds of malicious apps on Google Play that successfully bypassed Android 13’s security features, exposing users to malware, spyware, and data theft.

The apps exploited loopholes in permission handling and accessibility features, allowing them to steal credentials, track user activity, and install additional payloads.

This discovery underscores ongoing concerns about Google Play’s vetting process and the need for stronger app security policies, regular audits, and user vigilance to prevent malware from infiltrating mobile ecosystems.

Cybersecurity Advisors Network

NEWS:

24. Microsoft Exchange Online outage affects Outlook web users

Original Source: BleepingComputer by Sergiu Gatlan

A widespread Microsoft Exchange Online outage has disrupted Outlook Web Access, leaving users unable to send or receive emails.

The issue, affecting businesses and individuals globally, has raised concerns about service reliability and redundancy in cloud-based email infrastructure.

Microsoft has acknowledged the problem and is working on a resolution, but the disruption highlights the risks of over-reliance on a single provider.

Organisations are advised to implement backup communication plans and review business continuity strategies to mitigate the impact of future cloud service outages.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

25. Home Affairs explores secure service edge

Original Source: itNews by Eleanor Dickinson

The Australian Department of Home Affairs is evaluating Secure Service Edge (SSE) solutions to enhance network security, cloud access, and data protection.

SSE combines zero-trust principles, secure web gateways, and cloud security measures to improve visibility and control over sensitive information.

This move aligns with efforts to modernise cybersecurity frameworks and reduce reliance on legacy infrastructure, ensuring government agencies can safeguard critical data while maintaining seamless and secure access to cloud-based services.

The evaluation underscores the growing need for adaptive security solutions in government operations.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

26. CISA urges fired probationary workers to respond after federal judge grants order

Original Source: Cybersecurity Dive by David Jones

CISA is urging former probationary employees to respond after a federal judge ruled in their favour, granting an order that may allow them to reclaim their positions.

The ruling follows allegations that these employees were wrongfully terminated, raising concerns about hiring practices and workforce protections in federal cybersecurity roles.

While CISA has not disclosed full details, the case underscores broader issues around job stability, due process, and talent retention in critical security agencies.

Affected workers are encouraged to take action promptly to explore reinstatement options.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

27. Chinese Hackers Target European Diplomats with Malware

Original Source: ISMG Data Breach Today by Prajeet Nair

A Chinese state-sponsored hacking group is targeting European diplomats with custom malware, aiming to conduct espionage and extract sensitive information.

The attackers use phishing emails and compromised websites to deliver malware that provides persistent access to infected systems, enabling long-term surveillance.

Security experts warn that government agencies and international organisations must strengthen defenses, implement zero-trust policies, and enhance threat intelligence sharing to counter nation-state cyber threats and prevent diplomatic data breaches.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

28. RansomHub using FakeUpdates scheme to attack government sector

Original Source: Cybersecurity Dive by Rob Wright

The RansomHub ransomware group is leveraging the FakeUpdates (SocGholish) malware to infiltrate government networks, disguising malicious payloads as legitimate software updates.

Once installed, the malware enables data theft, system encryption, and extortion, forcing agencies to either pay ransoms or risk major operational disruptions.

The campaign highlights the growing use of social engineering in ransomware attacks, reinforcing the need for strict software update policies, advanced threat detection, and employee training to prevent falling victim to deceptive update schemes.

CyberSecurity Advisors Network

NEWS:

29. Meta vows to curtail false content, deepfakes ahead of Australian election

Original Source: itNews

With Australia’s upcoming elections, Meta has pledged to crack down on false content and deepfakes, aiming to curb misinformation and election interference.

The company is enhancing detection tools, working with fact-checkers, and increasing transparency measures to prevent AI-generated disinformation from influencing voters.

However, critics argue that enforcement remains inconsistent and that stronger regulatory oversight is needed.

The initiative underscores the growing role of AI in disinformation campaigns and the ongoing struggle between tech platforms, governments, and election security experts to protect democratic processes.

CyAN Cybersecurity Advisors Network

NEWS:

30. Curious tale of two HR tech unicorns, alleged espionage, and claims of a spy hiding in a bathroom

Original Source: The Register by Thomas Claburn

A bizarre corporate espionage saga has emerged between two rival HR tech unicorns, involving allegations of trade secret theft, covert surveillance, and even a spy hiding in a bathroom to gather intelligence.

The case, now unfolding in legal battles, underscores the high-stakes nature of data security in competitive industries.

Beyond the headline-grabbing drama, the incident highlights the growing risks of insider threats, corporate espionage, and cybersecurity failures, reinforcing the need for robust access controls, employee monitoring policies, and strict data protection measures in high-growth tech firms.

CyberSecurity Advisors Network

Webinaire : La relation de confiance entre le Data Protection Officer (DPO) et le Hacker Éthique

Nous avons le plaisir de vous inviter à un webinaire exclusif organisé dans le cadre de l’initiative Black Is Ethical, qui explorera une collaboration stratégique essentielle : la relation de confiance entre le Data Protection Officer (DPO) et le Hacker Éthique ou Construire une synergie efficace entre DPO et Hacker Éthique

📅 **26 Mars, 2025 | 🕒 11:00 CET**
💻 **En ligne (lien transmis après confirmation)**

🎙️ **Intervenants**
🔷 **Inssata RICOURT** – CISO & DPO, Fondateur de Black Is Ethical
🔷 **Lara ALOUAN** – Chercheuse en sociologie, Orange
🔷 **Yassir KAZAR** – CEO & Co-Founder, Yogosha
🔷 **Étienne COUPRIE – DPO de SogeCap**
🔷 **Léon MEIZOU – Ingénieur, Spécialiste en répression de la cybercriminalité, Chercheur en Sécurité pour NASA en matière de Cybersécurité.**
🎤 **Jean-Christophe le Toquin, Président de Cybersecurity Advisors Network (CyAN), Modérateur**

🚀 **Pour plus d'informations et inscription, cliquez sur le code QR ci-dessus!**

Cybersecurity Advisors Network

ANALYSIS:

31. Through the Lens of Music: What Cybersecurity Can Learn From Joni Mitchell

Original Source: SecurityWeek by Joshua Goldfarb

Cybersecurity, like music, thrives on balance, improvisation, and adaptability—lessons that Joni Mitchell's approach to songwriting can teach security professionals.

Just as Mitchell defied conventions by using unconventional tunings and evolving styles, cybersecurity must embrace flexibility, creativity, and a proactive mindset to counter evolving threats.

The article explores how risk management, defence strategies, and security innovation benefit from a holistic approach, reinforcing that effective cybersecurity is both an art and a science, requiring intuition, structure, and the ability to adapt to an unpredictable landscape.

Cybersecurity Advisors Network

ANALYSIS:

32. 5 Identity Threat Detection & Response Must-Haves for Super SaaS Security

Original Source: The Hacker News

As identity-based attacks surge, security experts highlight five critical components of effective Identity Threat Detection & Response (ITDR) for SaaS environments.

These include continuous identity monitoring, behavioural analytics, adaptive authentication, automated response mechanisms, and strong integration with existing security frameworks.

With attackers increasingly targeting identity as the weakest link, organisations must prioritise identity-centric security strategies to prevent unauthorised access, account takeovers, and data breaches in cloud-based applications.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

33. Why Cybersecurity Needs More Business-Minded Leader

Original Source: Dark Reading by Victoria Dimmick

Cybersecurity is no longer just a technical challenge—it's a business imperative. Experts argue that CISOs and security leaders must adopt a business mindset, aligning security strategies with organisational goals, risk management, and financial impact.

Too often, cybersecurity is seen as a cost centre rather than a driver of trust, resilience, and competitive advantage.

To bridge this gap, security leaders must improve communication with executives, translate technical risks into business language, and integrate cybersecurity into overall corporate strategy to ensure long-term success.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

34. How Governments and Businesses in Canada and the EU Can Reduce Dependence on U.S.-Controlled Cloud Infrastructure

Original Source: PrivID (Substack)

With concerns over data sovereignty and regulatory control, governments and businesses in Canada and the EU are exploring ways to reduce reliance on U.S.-controlled cloud infrastructure.

Current cloud dependencies expose sensitive data to foreign surveillance laws and jurisdictional risks, prompting calls for localised, sovereign cloud solutions.

Experts emphasise the need for investment in regional cloud providers, stricter data residency policies, and regulatory frameworks that ensure compliance with privacy laws while maintaining competitive access to cloud-based innovation.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

35. Zhou Shuai: A Hacker's Road to APT27

Original Source: Natto Thoughts by the Natto Team

The story of Zhou Shuai, an infamous hacker linked to APT27, offers an inside look into the rise of one of the most notorious Chinese cyber espionage groups.

Zhou's journey from small-time attacks to orchestrating large-scale campaigns targeting global industries and governments highlights the increasing sophistication of state-backed cyber operations.

This analysis explores the tactics, techniques, and procedures (TTPs) used by APT27, emphasising the need for organisations to implement advanced threat detection, improved intelligence-sharing, and a more aggressive approach to identifying and defending against these persistent threats.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

ANALYSIS:

36. Sovereign digital infrastructure. Will Australia seize the moment?

Original Source: InnovationAus by Rupert Taylor-Price

As digital sovereignty becomes a growing concern, Australia faces a critical decision—should it invest in nationally controlled digital infrastructure or continue relying on foreign technology providers?

With increasing risks from geopolitical tensions, data privacy laws, and supply chain vulnerabilities, experts argue that developing sovereign cloud solutions, local data centres, and secure communication networks is essential for economic security and resilience.

However, achieving this requires strong policy frameworks, public-private collaboration, and significant investment to reduce dependence on global tech giants while maintaining competitiveness.

For more on this subject see Article 38: 'Navigating Uncharted Waters: The EU's Digital Markets Act and Its Impact on Security' by CyAN's Kim Chandler McDonald

CyAN Cybersecurity Advisors Network

ANALYSIS:

37. The EU General Data Protection Regulation: A Commentary (2nd edition)

Original Source: Oxford University Press Edited by Christopher Kuner, Lee A. Bygrave & Christopher Docksey

The second edition of the EU General Data Protection Regulation (GDPR) commentary provides an in-depth analysis of the regulation's evolving impact on privacy, compliance, and data protection frameworks.

As enforcement actions increase and global companies adjust to stricter regulations, the book examines legal interpretations, case studies, and ongoing challenges faced by businesses operating under GDPR.

With data privacy laws influencing policies worldwide, this edition offers valuable insights for lawmakers, compliance officers, and security professionals navigating the complexities of modern data protection.

CyberSecurity Advisors Network

CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Have you got what it takes to outsmart your fellow cybersecurity pros? It’s time to put your skills to the test in our Quarterly #CyANQuiz Challenge, kicking off on March 31st!

🔷 30 Questions. Timed. No second chances.
🔷 Based on Recent Cybersecurity News & Events – Watch out for recent news and Cybersecurity events.

📅 **Check your email on March 31st for the quiz link**; just click, answer, and climb the leaderboard!
💡 Why Play? Compete, have fun, and win awesome prizes (while proving your cybersecurity dominance!

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

Think you can take the cyber crown? Prove it!

CyAN CyAN Members
Op Eds, Articles, etc

38. Navigating Uncharted Waters: The EU's Digital Markets Act and Its Impact on Security

By CyAN Global Vice President, Kim Chandler McDonald

In this article Kim explores the far-reaching implications of the EU’s Digital Markets Act (DMA) on cybersecurity, highlighting how the legislation aims to curb monopolistic practices, enhance digital competition, and introduce stricter security standards for major tech platforms.

While the DMA promotes data privacy and transparency, it also raises questions about enforcement, compliance burdens, and unintended security risks.

Kim emphasises the need for businesses to adapt, regulators to stay vigilant, and cybersecurity leaders to anticipate both challenges and opportunities as the EU reshapes the digital landscape.

CyberSecurity Advisors Network

39. “What Happens to Heroes?” – EPISODE #2: The Unsung Heroes of the Digital World

By CyAN member, Anidris IT Advisor/Data Protection Officer, and Author, Didier Annet

In his latest ‘episode’ Didier shines a light on the often-overlooked cybersecurity professionals who work tirelessly behind the scenes to defend systems, data, and digital infrastructure. While cyber threats make headlines, those who prevent breaches, mitigate attacks, and secure critical assets rarely get recognition.

This piece explores the mental and emotional toll of frontline defenders, the lack of visibility for their contributions, and the need for stronger industry support, acknowledgment, and resilience strategies to ensure these unsung heroes remain motivated and protected in an increasingly hostile digital world.

Without greater recognition and investment in their well-being, burnout and attrition threaten to weaken the very defenses organizations rely on. As cyber threats grow more sophisticated, ensuring the people behind the screens are valued and supported is just as critical as strengthening the technology itself.

40. Securing the Future: Innovative Cybersecurity for Agentic AI

By CyAN Member RSA Conference Blob by Shantanu Bhattacharya

In this exploration of cybersecurity's next frontier, Shantanu examines the risks and safeguards needed for Agentic AI—a new class of AI systems capable of autonomous decision-making and adaptive learning.

As these models become more independent, traditional security frameworks struggle to keep pace. Shantanu highlights the need for proactive threat modelling, robust governance, and ethical safeguards to ensure these systems remain secure, accountable, and resistant to adversarial manipulation, reinforcing that cybersecurity must evolve alongside AI innovation.

Without rigorous oversight, Agentic AI could introduce unpredictable security risks, from data poisoning to unauthorised decision-making that impacts critical systems. By embedding cybersecurity into AI's foundation, organizations can harness its potential while mitigating the unintended consequences of unchecked autonomy.

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!

Don't miss CyAN Global VP Kim Chandler McDonald on Risky Women Radio!

In the captivating 'Risk and Compliance Against Technology-Facilitated Domestic Violence' episode, Kim shares her journey from theatre to becoming the co-founder and CEO of 3 Steps Data—and our VP!

She delves into her advocacy for proactive compliance and robust risk strategies to protect vulnerable users, democratising technology, and combating technology-facilitated domestic violence.

Kim also underscores the critical role of end-to-end encryption in ensuring data security and privacy. Alongside, she regales with tales from interviewing global leaders to her adventurous stint as an emergency forest firefighter!

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!

The first-ever CyAN APAC Community Call brought together 10 members for an intimate and insightful discussion.

John Salomon and Saba Bagheri shared mentorship experiences and what mentees need most.

The conversation naturally shifted to certifications vs. experience in cybersecurity, led by Ned Farhat, with thoughtful input from Joe Cozzupoli, Fatema Fardan, and others.

Saba also invited Fatema to join the March "Women in Cyber" feature. The group proposed a webinar: "Seeking a Job in Cybersecurity? The Questionable Value of Certifications." A warm, engaging call overall!

CyAN thrives because of the incredible talent, leadership, and dedication of our members; we are always immensely pleased to foster communication, cooperation and collaboration between then as we work together to craft the future of cybersecurity on a global stage! 🚀💙

CyAN Cybersecurity Advisors Network

UPCOMING CyAN and CyAN Partner EVENTS:

- Trust & Safety Forum at Forum INCYBER Europe (FIC), Lille, France: April 1-2 https://tinyurl.com/mrruerfz
- Supply Chain Cyber Security Summit (SCCS), Lisbon Portugal: 9-11 April 2025 https://sccybersecurity.com/cyber-security-summit-europe/
- GITEX AFRICA, Marrakesh, Morocco: 14-16 April https://tinyurl.com/2yhuztwk
- GITEX ASIA, Singapore (Marina Bay Sands: 23-25 April https://gitexasia.com/
- GISEC Global, Dubai World Trade Centre: 6-8 May https://gisec.ae/home
- The Cyber Outstanding Security Performance Awards (Cyber OSPAs), London, UK: 8 May https://www.thecyberospas.com/about/
- CSG Awards 2025, Dubai: 7 May https://csgawards.com/
- World AI Technology Expo, Dubai: 14-15 May https://worldaiexpo.i
- CyAN 10th Anniversary Celebrations!
- GITEX Europe Messe, Berlin: 21-23 May https://www.gitex-europe.com/
- MaTeCC, Rabat, Morocco: 7-9 June https://tinyurl.com/mtecz8vw
- CyAN Q2 Community Call (APAC and the Gulf), June 11: 12:00 GST / 16:00 SGT / 18:00 AEST
- CyAN Q2 Community Call (EMEA and the Americas), June 11: 20:00 GST / 18:00 CET / 17:00 UTC / 12:00 EDT

CyAN Cybersecurity Advisors Network

Bookings Open for the 2025 Cyber OSPAs

Tickets Available till March 26th!

🚀 **And the finalists are…**

The entries are in, the judges have deliberated, and the finalists have been revealed. Now, it's time for the grand finale—the moment we celebrate the best and brightest in cybersecurity!

On 8th May 2025, under the dazzling lights of 133 Houndsditch, London, the Big SASIG Conference Dinner will set the stage for an unforgettable evening of recognition, inspiration, and industry camaraderie.

Who will take home the top honours? Which names will be etched into cybersecurity history? Be there to witness the triumphs, toast to excellence, and celebrate the incredible individuals driving our industry forward!

2025 Cyber OSPAs

Winners of the 2025 Cyber OSPAs will be revealed on Thursday 8th May

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