CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #136

NEWS:

1. Italian government approved use of spyware on members of refugee NGO, MPs told

Original Source: The Guardian by Angela Giuffrida & Stephanie Kirchgaessner

Italian lawmakers have been informed that spyware was authorised against members of a refugee NGO, sparking fierce backlash over potential human rights violations.

Critics argue this blurs the line between national security and the criminalisation of humanitarian work.

The use of surveillance tools on aid workers raises serious concerns about transparency, oversight, and democratic accountability.

It also reignites broader debates on the unchecked proliferation of spyware in democratic societies and its chilling effect on civil society, dissent, and freedom of expression.

CyberSecurity Advisors Network

NEWS:

2. How CISA Cuts Impact Election Security

Original Source: Dark Reading by Alexander Culafi

Budget cuts to CISA are raising alarms ahead of the U.S. election season, with experts warning that downsizing critical cyber defences could leave electoral infrastructure vulnerable.

The agency plays a vital role in helping states defend against disinformation, phishing campaigns, and nation-state meddling — all of which are expected to escalate.

Reducing CISA’s capacity now not only limits real-time response capabilities but also undermines public trust.

With threats evolving, the need for robust, well-funded cyber readiness has never been more urgent — especially when democratic legitimacy is on the line.

CyberSecurity Advisors Network

NEWS:

3. Mozilla warns Windows users of critical Firefox sandbox escape flaw

Original Source: BleepingComputer buy Sergiu Gatlan

A newly disclosed Firefox vulnerability allows attackers to bypass the browser’s sandbox protections on Windows, exposing users to significant risk.

The flaw could let malicious code execute with elevated privileges, opening the door to full system compromise when paired with other exploits. Mozilla has issued patches and urges users to update immediately.

This incident underscores how even widely trusted tools can harbour critical flaws—and how attackers continue to target popular software used by millions.

Regular patching and layered defences remain essential in mitigating zero-day threats.

CyberSecurity Advisors Network

NEWS:

4. New Morphing Meerkat Phishing Kit Mimics 114 Brands Using Victims' DNS Email Records

Original Source: The Hacker News by Ravie Lakshmanan

A sophisticated phishing kit dubbed “Morphing Meerkat” has been spotted in the wild, leveraging victims’ own DNS email records to convincingly impersonate more than 100 well-known brands.

This dynamic attack method enables real-time spoofing, tricking recipients into trusting fraudulent emails with alarming accuracy.

By tailoring each message to align with the recipient’s existing email infrastructure, the kit bypasses traditional detection methods and increases the likelihood of successful compromise.

Organisations are urged to review DNS configurations, implement strict email authentication protocols like DMARC, and educate users to spot red flags in even the most convincing emails.

CyberSecurity Advisors Network

NEWS:

5. Security shop pwns ransomware gang, passes insider info to authorities

Original Source: The Register by Connor Jones

In a bold counteroffensive, cybersecurity firm Halcyon turned the tables on a ransomware gang by infiltrating their operations and relaying critical intel to law enforcement.

The gang in question, involved in high-profile attacks under various aliases like Arcus Media and Volcano Demon, has been using advanced ransomware variants to target enterprises globally.

Halcyon’s efforts exposed tools, payment structures, and infrastructure used by the criminals, aiding investigations.

This proactive move not only disrupted ongoing campaigns but also highlighted the growing role private sector defenders play in hunting threat actors. It's a rare but powerful win for the good guys.

CyberSecurity Advisors Network

NEWS:

6. UK Software Firm Fined £3 Million Over Ransomware-Caused Data Breach

Original Source: SecurityWeek by Eduard Kovacs

A UK software company has been hit with a £3 million fine after a ransomware attack led to a significant data breach, exposing personal and sensitive information.

Regulators found the firm failed to implement adequate cybersecurity measures, including proper access controls and regular risk assessments—despite having previously identified critical vulnerabilities.

The fine underscores how regulatory bodies are tightening scrutiny around ransomware readiness and response. It also sends a clear message: neglecting basic cyber hygiene can lead to financial and reputational fallout far beyond the ransom demand.

Prevention, not just reaction, is key.

CyberSecurity Advisors Network

NEWS:

7. Hackers Repurpose RansomHub's EDRKillShifter in Medusa, BianLian, and Play Attacks

Original Source: he Hacker News by Ravie Lakshmanan

Cybercriminals have adapted RansomHub's EDRKillShifter tool for use in high-profile ransomware campaigns by Medusa, BianLian, and Play.

This repurposed tool is designed to neutralise endpoint detection and response (EDR) systems, making it easier for attackers to encrypt data and evade detection. Its modular design allows threat actors to target a wide range of systems, suggesting a growing level of collaboration or shared tooling among ransomware groups.

The trend highlights how the ransomware ecosystem is evolving, with advanced techniques being recycled and rebranded for new campaigns—escalating the cat-and-mouse game between attackers and defenders.

CyberSecurity Advisors Network

NEWS:

8. SignalGate Isn’t About Signal

Original Source: Wired by Andy Greenberg & Lily Hay Newman

Despite headlines suggesting otherwise, the so-called “SignalGate” controversy has little to do with the Signal messaging app itself.

At the heart of the story is a national security blunder: high-ranking U.S. officials shared classified military intelligence via Signal—but the issue wasn't the app’s encryption.

It was the human error and poor judgement in using any messaging platform to share sensitive content in the first place.

The coverage serves as a potent reminder that even the most secure tools can’t compensate for bad operational security. In this case, the real breach wasn't in technology—it was in trust and protocol.

CyberSecurity Advisors Network

NEWS:

9. Fake DeepSeek Ads Spread Malware to Google User

Original Source: Dark Reading by Rob Wright

A malicious ad campaign is impersonating legitimate DeepSeek content to target Google users, distributing malware through carefully crafted phishing lures.

Victims are enticed by ads that appear genuine, only to be redirected to sites hosting malware that can steal data or compromise systems.

This attack highlights how even trusted ad networks can be manipulated by threat actors and underscores the risks associated with search engine advertising.

As attackers continue to blend social engineering with technical deception, users are urged to verify URLs and avoid downloading content from unfamiliar sources—no matter how legitimate it looks on the surface.

CyberSecurity Advisors Network

NEWS:

10. Threat actor in Oracle Cloud breach may have gained access to production environments

Original Source: Cybersecurity Dive by David Jones

A threat actor behind a recent Oracle Cloud breach may have infiltrated production environments, raising serious concerns about the extent of access and potential data exposure.

Investigators are still piecing together the timeline, but evidence suggests that compromised credentials allowed lateral movement within the environment.

The incident illustrates the dangers of credential misuse in cloud ecosystems and the critical need for layered defences, robust access controls, and continuous monitoring.

As cloud dependencies grow, so does the risk—making it essential for organisations to reassess their cloud security posture before attackers find their way in.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

Celebrating International Women in Tech Day on April 4th!

Behind the Keys:

Women Who Secure the Future

Next week, CyAN shines a spotlight on some of the amazing women who protect what matters

Check in daily to read the stories of strength, strategy, and service — told by the women behind the keys!

NEWS:

11. New Atlantis AIO platform automates credential stuffing on 140 services

Original Source: BleepingComputer by Bill Toulas

The Atlantis AIO platform represents a major shift in cybercrime, offering an automated solution for credential stuffing across a vast range of 140 services, including banks, email providers, and VPNs.

This tool dramatically simplifies the process for cybercriminals to test and exploit stolen credentials efficiently, with advanced evasion techniques that minimise detection. It continuously updates to adapt to new security measures, making it a persistent threat.

The rise of Atlantis AIO underscores the urgent need for enhanced defensive strategies across all digital platforms to counteract the growing ease of conducting large-scale fraud operations.

CyberSecurity Advisors Network

NEWS:

12. OpenAI Offering $100K Bounties for Critical Vulnerabilities

Original Source: SecurityWeek by Ryan Naraine

OpenAI is offering bounties of up to $100,000 for critical vulnerabilities, reinforcing the vital role of responsible disclosure in safeguarding AI systems.

As generative models become more embedded in sensitive operations, the stakes for security have never been higher.

This initiative rewards researchers for identifying flaws that could lead to data leaks, prompt injection attacks, or unauthorised model manipulation.

It also signals growing awareness that AI products, like any tech, require continuous testing, ethical oversight, and community involvement to remain secure at scale.

CyberSecurity Advisors Network

NEWS:

13. New Readerupdate Malware Variants Target MacOS Users

Original Source: Security Affairs by Pierluigi Paganini

New ReaderUpdate malware variants are targeting macOS users with heightened stealth and persistence.

These strains masquerade as legitimate software updates, tricking victims into granting access that enables full system compromise. Once installed, the malware can monitor activity, steal credentials, and evade detection through rootkit-like behaviour.

Security researchers warn that this marks a worrying escalation in macOS-targeted campaigns, reinforcing the need for vigilant patching, strict download practices, and robust endpoint protection—even in ecosystems traditionally seen as safer.

CyberSecurity Advisors Network

NEWS:

14. INTERPOL Arrests 306 Suspects, Seizes 1,842 Devices in Cross-Border Cybercrime Bust

Original Source: The Hacker News by Ravie Lakshmanan

INTERPOL's latest operation has led to the arrest of 306 individuals and the seizure of nearly 2,000 devices in a sweeping international crackdown on cybercrime.

Coordinated across 55 countries, the operation targeted a wide range of digital threats, including ransomware, phishing, and online fraud.

Authorities also identified over 1,300 suspicious IP addresses and dismantled numerous criminal infrastructure networks.

This effort highlights the growing success of international law enforcement collaboration in tracking and disrupting cybercriminal operations, reinforcing the importance of cross-border threat intelligence and resource sharing.

CyberSecurity Advisors Network

NEWS:

15. Private Data and Passwords of Senior U.S. Security Officials Found Online

Original Source: Spiegel International by Patrick Beuth, Jörg Diehl, Roman Höfner, Roman Lehberger, Friederike Röhreke & Fidelius Schmid

An alarming investigation has revealed that the personal data and passwords of high-ranking U.S. security officials—some still in office—were freely available on the dark web.

The compromised credentials, including those from official government platforms, were traced back to widespread data leaks and poor credential hygiene.

The findings underscore the persistent risks of credential stuffing, the failure of password reuse policies, and the absence of strong multi-factor authentication.

This incident is a stark reminder that even national security leaders are vulnerable if basic cybersecurity practices aren't rigorously enforced and continuously monitored.

CyberSecurity Advisors Network

NEWS:

16. DOGE staffer 'Big Balls' provided tech support to cybercrime ring

Original Source: itNews Raphael Sagger

New revelations suggest that a DOGE-affiliated staffer, known only by the handle “Big Balls,” provided hands-on technical support to a notorious cybercrime ring.

This staffer allegedly assisted in developing and troubleshooting the systems used to distribute malware and conduct illicit online activities.

The involvement of someone from a federally linked entity raises critical questions about internal oversight, trust, and the porous boundaries between official platforms and malicious operations.

This case highlights the urgent need for rigorous vetting, continuous monitoring, and transparent accountability for those operating within or adjacent to sensitive digital ecosystems.

CyberSecurity Advisors Network

NEWS:

17. Files stolen from NSW court system, including restraining orders for violence

Original Source: The Register by Connor Jones

A data breach within the NSW court system has led to the exposure of sensitive legal documents, including restraining orders tied to domestic violence cases.

The breach has alarmed privacy advocates and legal professionals, given the highly personal nature of the leaked information and the potential for real-world harm to victims.

Authorities are investigating how the breach occurred and whether security failings enabled unauthorised access.

This incident underscores the critical importance of securing judicial data, especially where the safety of vulnerable individuals may be directly compromised.

CyberSecurity Advisors Network

NEWS:

18. Trump signs executive order that will upend US voter registration processes

Original Source: The Guardian by Joseph Gedeon & Sam Levine

A sweeping executive order signed by Donald Trump threatens to dramatically reshape how voter registration is handled across the United States.

The order includes provisions that critics argue could suppress voter turnout, particularly among marginalised communities, by tightening verification requirements and limiting digital registration options.

Civil liberties groups have voiced concern over the implications for election accessibility and integrity.

As the US heads into another contentious election cycle, the move is expected to prompt legal challenges and intensify debates over democratic participation and electoral security.

CyberSecurity Advisors Network

NEWS:

19. Secretive Chinese network tries to lure fired US gov workers

Original Source: itNEWS by AJ Vicens

A covert influence campaign linked to China is targeting recently dismissed U.S. government employees, aiming to exploit their insider knowledge and access.

The campaign uses job offers and recruitment outreach as a front, hoping to gather sensitive information or sway opinion in Beijing’s favour.

National security experts warn that such operations highlight the risks posed by abrupt personnel changes, especially in critical sectors like defence and cybersecurity.

This development underscores the need for robust post-employment protocols and greater awareness of foreign interference tactics.

CyberSecurity Advisors Network

NEWS:

20. Using Starlink Wi-Fi in the White House Is a Slippery Slope for US Federal IT

Original Source: Wired by Lily Hay Newman

Concerns are mounting over the potential use of Starlink Wi-Fi within sensitive U.S. government settings like the White House.

While the satellite service offers reliable internet, its proprietary infrastructure and lack of transparency raise red flags about data sovereignty, control, and vulnerability to surveillance or disruption.

Security experts caution that relying on non-government-managed networks—especially those linked to powerful private entities—introduces significant risks to national cybersecurity.

The situation calls for clearer federal policies around external tech integration and digital autonomy.

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!

NEWS:

21. OTF, which backs Tor, Let's Encrypt and more, sues to save funding from Trump cuts

Original Source: The Register by Thomas Claburn

The Open Technology Fund (OTF)—a key supporter of privacy-enhancing tools like Tor and Let's Encrypt—has launched legal action to protect its funding, which is threatened by proposed Trump-era budget cuts.

OTF argues the cuts would weaken digital rights efforts globally and endanger activists, journalists, and at-risk communities who rely on secure communication platforms.

The lawsuit underscores the essential role of publicly funded, open-source technologies in defending internet freedom.

As global threats to online privacy grow, the outcome of this legal battle could have far-reaching implications for the future of secure digital infrastructure.

CyberSecurity Advisors Network

NEWS:

22. Critical Ingress NGINX Controller Vulnerability Allows RCE Without Authentication

Original Source: The Hacker News by Ravie Lakshmanan

A newly disclosed vulnerability in the NGINX Ingress Controller for Kubernetes could allow remote code execution without authentication—posing a significant threat to cloud-native environments.

The flaw, dubbed “IngressNightmare,” stems from improper handling of annotations and affects multiple versions widely deployed in production. If exploited, it could let attackers execute arbitrary code, compromise workloads, and escalate privileges within clusters.

Security teams are urged to apply patches immediately and review ingress configurations for exposure.

As Kubernetes adoption grows, securing its control planes becomes essential to maintaining resilience in increasingly containerised infrastructure.

CyberSecurity Advisors Network

NEWS:

23. Top Trump officials text classified Yemen airstrike plans to journo in Signal SNAFU

Original Source: The Register by Iain Thomson

A major operational security lapse has come to light involving former Trump officials, who reportedly shared classified details of Yemen airstrikes via Signal with a journalist.

The messages—containing sensitive military plans—were part of a broader communication exchange that raises serious questions about mishandling of classified information and the misuse of encrypted messaging apps.

While Signal itself remains secure, the incident underscores how poor operational judgment—not just technical flaws—can lead to critical breaches.

Experts warn that trust in encryption tools can't compensate for user behaviour that disregards basic security protocols, especially in government and defence circles.

CyberSecurity Advisors Network

NEWS:

24. New VanHelsing ransomware targets Windows, ARM, ESXi systems

Original Source: BleepingComputer by Bill Toulas

A newly identified ransomware strain, VanHelsing, is making waves by targeting a diverse array of systems—including Windows, Linux on ARM, and VMware ESXi.

This multi-platform approach allows attackers to cast a wider net, increasing their ability to disrupt operations across hybrid environments.

Researchers say the ransomware uses a variety of obfuscation techniques and custom scripts to evade detection and escalate privileges before encrypting files.

Its wide compatibility highlights a growing trend among cybercriminals to design attacks that can bypass traditional defences and strike where visibility is weakest.

As hybrid infrastructure becomes the norm, organisations are urged to revisit their endpoint security, backup policies, and threat detection capabilities.

CyberSecurity Advisors Network

NEWS:

25. Critical 'IngressNightmare' Vulns Imperil Kubernetes Environments

Original Source: Dark Reading by Jai Vijayan

"IngressNightmare"—is sending shockwaves through the Kubernetes community. These flaws affect the NGINX Ingress Controller, a widely used component in Kubernetes clusters, and allow remote code execution without authentication under certain configurations.

With widespread usage across production environments, the exposure risk is significant, especially for organisations that have not implemented strict access controls.

The discovery has prompted urgent calls for patching, configuration reviews, and broader Kubernetes security hygiene.

As container orchestration grows in popularity, so too does its attractiveness to attackers, highlighting the need for continuous monitoring, rapid patch deployment, and a deeper focus on securing the cloud-native stack.

CyberSecurity Advisors Network

NEWS:

26. Cyberattack takes down Ukrainian state railway's online services

Original Source: BleepingComputer by Bill Toulas

A cyberattack has disrupted the online services of Ukrainian state railway operator Ukrzaliznytsia, affecting ticket purchasing and passenger information systems.

While operations on the ground continue, the digital shutdown poses a serious inconvenience to travellers and reflects broader cyber risks targeting critical infrastructure in conflict zones.

Ukrainian authorities suspect state-aligned threat actors, consistent with past patterns of cyber aggression amid the ongoing war.

The incident highlights the vulnerability of national transport systems to digital sabotage and underscores the importance of investing in resilient infrastructure and contingency planning.

As geopolitical tensions continue, public services must prioritise cybersecurity as a frontline defence.

CyberSecurity Advisors Network

NEWS:

27. Canadian citizen allegedly involved in Snowflake attacks consents to extradition to US

Original Source: Cyberscoop by Matt Kapko

A Canadian national accused of involvement in the high-profile Snowflake data theft campaign has agreed to extradition to the United States.

Authorities believe the individual was linked to cyberattacks that compromised multiple companies by exploiting misused credentials and cloud services.

The decision marks a step forward in cross-border cooperation to hold cybercriminals accountable.

As breaches grow in scale and complexity, this case underscores the global nature of cybercrime and the mounting pressure on legal systems to keep pace with threats exploiting cloud infrastructure and identity-based vulnerabilities.

CyberSecurity Advisors Network

NEWS:

28. Enhancing Threat Intelligence and Threat Detection in Australian Central Government Organisations

Original Source: IT Wire by Cyrille Badeau

Australian central government agencies are under increasing pressure to modernise their cybersecurity practices, with real-time threat detection and AI-driven intelligence now essential for identifying and countering sophisticated attacks.

Traditional perimeter defences are no longer sufficient—agencies must embrace advanced analytics, automation, and behavioural insights to stay resilient.

Visibility across complex IT environments is critical, along with a proactive, intelligence-led approach that aligns security strategies with today's evolving threat landscape and heightened policy expectations.

CyberSecurity Advisors Network

NEWS:

29. How to delete your 23andMe data and why you should do it now

Original Source: ZDNet by Steven Vaughan-Nichols

Following last year’s breach that exposed the genetic data of millions, 23andMe is again under fire for its data handling practices.

Users are now being urged to permanently delete their personal and genetic information, with clear steps provided for doing so.

With sensitive DNA profiles potentially accessed by law enforcement or third parties via platform loopholes, the risks of leaving data behind are mounting.

While deletion can’t guarantee total erasure, it significantly limits future exposure and prompts a critical re-evaluation of trust in consumer genetics services.

CyberSecurity Advisors Network

NEWS:

30. Amazon ends little-used privacy feature that let Echo users opt out of sending recordings to company

Original Source: The Associated Press

Amazon has quietly discontinued a privacy option that allowed Echo users to opt out of having their voice recordings reviewed by the company.

The feature, introduced after backlash over human review of Alexa interactions, is no longer available—raising fresh concerns about transparency and user control.

While Amazon claims it still limits how recordings are used, privacy advocates argue the move erodes trust and limits meaningful consent.

As voice assistants become more embedded in everyday life, users may want to rethink how much they're willing to share with their smart devices.

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!**

ANALYSIS:

31. Explain Signal, cybersecurity, and how a journalist was sent high-level military intelligence

Original Source: Virginia Tech News with France Bélanger, Aaron Brantly, Jimmy Ivory & Anthony Vance

When Atlantic editor-in-chief Jeffrey Goldberg unexpectedly received classified military plans via Signal, it exposed how encrypted messaging can be both a shield and a sword.

The incident raises critical questions about digital trust, secure communications, and insider threats.

While apps like Signal are essential for privacy, they also complicate traditional information controls.

This analysis explores how governments and media must rethink cybersecurity training and access protocols, ensuring that encryption empowers democracy without unintentionally bypassing national security safeguards.

CyberSecurity Advisors Network

ANALYSIS:

32. Improving cybersecurity to protect against online hate

Original Source: Harvard School of Public Health by Jay Lay

Online hate is on the rise, yet cybersecurity strategies often overlook its role in fuelling real-world violence.

This fascinating piece explores how hate-fuelled digital abuse transcends mere content moderation, requiring stronger security protocols to shield targets from harassment, doxxing, and coordinated attacks.

It highlights the need for an interdisciplinary approach—combining tech, policy, and public health—to build safer platforms.

Addressing online hate isn’t just about protecting reputations; it’s about safeguarding mental health, social cohesion, and democratic discourse from digital weaponisation.

CyberSecurity Advisors Network

ANALYSIS:

33. Cybersecurity Gaps Leave Doors Wide Open

Original Source: Dark Reading by Jai Vijayain

Despite growing investment in cybersecurity, many organisations remain exposed due to fundamental oversights—such as misconfigured systems, weak identity management, and neglected patching routines.

These gaps are routinely exploited in ransomware, phishing, and supply chain attacks.

Security leaders are being urged to refocus on core cyber hygiene, ensuring that basic controls are prioritised alongside advanced tools.

In a threat environment where attackers thrive on preventable mistakes, resilience depends not on having the flashiest defences, but on the reliability of the essentials.

CyberSecurity Advisors Network

ANALYSIS:

34. Global Data Privacy Minefield

Original Source: PrivID (Substack)

Navigating global data privacy laws has become a regulatory tightrope walk.

With divergent standards between the EU, U.S., and emerging markets, organisations must juggle compliance obligations while maintaining operational efficiency.

This analysis explores the growing friction between localisation mandates and cross-border data flows, warning that inconsistent regulation threatens innovation and business continuity.

Without harmonised frameworks or updated treaties, companies face legal uncertainty and escalating costs. Clearer global alignment is essential to create a digital ecosystem where privacy rights are upheld without stifling economic growth.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

ANALYSIS:

35. Australia’s government agencies use encrypted messaging apps such as Signal. But should they?

Original Source: The Guardian by Josh Taylor & Josh Butler

The increasing reliance on encrypted messaging apps like Signal by Australian government agencies has sparked debate over security, transparency, and public accountability.

While these tools provide robust privacy and are vital for protecting sensitive communications, they also raise concerns about record-keeping obligations and public access to government decisions.

This piece explores the tension between national security needs and democratic oversight, questioning whether these apps are being used appropriately or risk circumventing proper governance. Striking the right balance is critical to maintaining trust and compliance in the digital age.

CyberSecurity Advisors Network

ANALYSIS:

36. When Cybersecurity Measures Backfire

Original Source: PrivID (Substack)

Not all security controls improve security—some can actually increase risk. Overly complex authentication, intrusive surveillance, or rigid access restrictions can frustrate users, encouraging risky workarounds or disengagement.

In high-stakes environments, such counterproductive measures undermine trust and resilience, making systems more fragile, not less.

This piece explores the paradox of protection, arguing that effective cybersecurity must be user-centred, context-aware, and flexible enough to adapt without compromising core defences.

Security isn’t about more controls—it’s about smarter, more human-focused ones.

CyberSecurity Advisors Network

ANALYSIS:

37. How to Enter the US With Your Digital Privacy Intact

Original Source: Wired by Andy Greenberg

Crossing the U.S. border with your digital devices can feel like navigating a surveillance minefield.

Authorities may search phones, demand passwords, or access cloud data—raising major privacy concerns for travellers, especially journalists and activists.

This guide outlines how to protect your digital footprint, from using burner devices and disabling biometric locks to limiting stored sensitive data and backing up securely beforehand.

Maintaining digital privacy at international borders isn’t just about evasion—it’s about preparation, precaution, and understanding your rights in a data-driven world.

CyberSecurity Advisors Network

ANALYSIS:

38. Is nation-state hacking becomes 'more in your face,' are supply chains secure?

Original Source: The Register by Jessica Lyons

The gloves are off—nation-state hacking is no longer covert, it’s confrontational.

As geopolitical tensions rise, adversaries are escalating cyber operations, targeting supply chains with brazen attacks that aim to destabilise critical infrastructure and erode trust.

With the SolarWinds and Microsoft Exchange attacks still casting long shadows, experts warn that many organisations remain underprepared for these sophisticated threats.

The piece calls for improved vendor scrutiny, real-time threat intelligence, and resilient architecture to withstand increasingly direct cyber onslaughts from well-resourced state actors.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

STATISTICS & INSIGHTS
powered by evisec

39. Highlights from this week's cybersecurity research by evisec - CRD #19

Original Source: CyAN Member and evisec CEO Henry Röigas

- Ransomware hits record high: February 2025 saw 962 victims—more than double the monthly average—with Cl0p behind one-third of cases.
- Credential compromise leads access: Nearly half of ransomware cases in 2024 began with compromised credentials, often via brute-force or weak MFA.
- Infostealers drive initial access market: 3.2 billion credentials were leaked in 2024, 75% linked to infostealers.
- Machine identities under attack: Half of surveyed firms faced breaches via exposed API keys or certificates; usage is rising fast.
- LLMs linked to secret leaks: GitHub repos using Copilot saw 40% more hardcoded secrets, highlighting AI-related security risks.

CyberSecurity Advisors Network

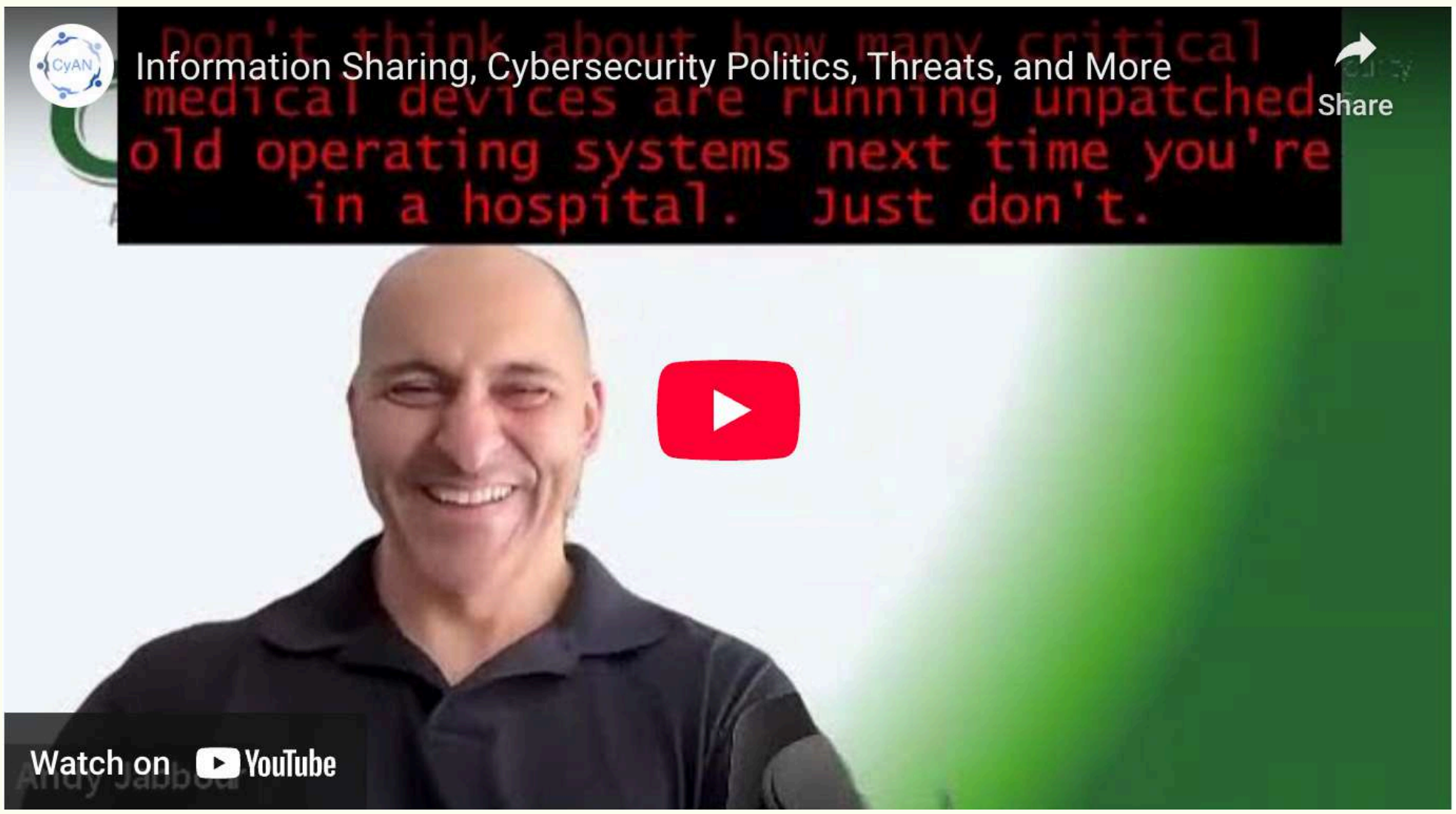
CyAN CyAN Members Op Eds, Articles, etc

CyAN Podcast: Infommation Sharing, Cyversecurity Politics, Threats and More!

Gate 15‘s Andy Jabbour joins CyAN’s Director of Communications, John Salomon on this episode of CyAN’s Secure-in-Mind series.

They discuss a wide variety of topics including information and intelligence sharing, geopolitics, US and European cybersecurity capabilities, information security investment, collective cyberdefence, adversaries, threats, and even some nifty travel tips.

Access the Podcast via the QR code above

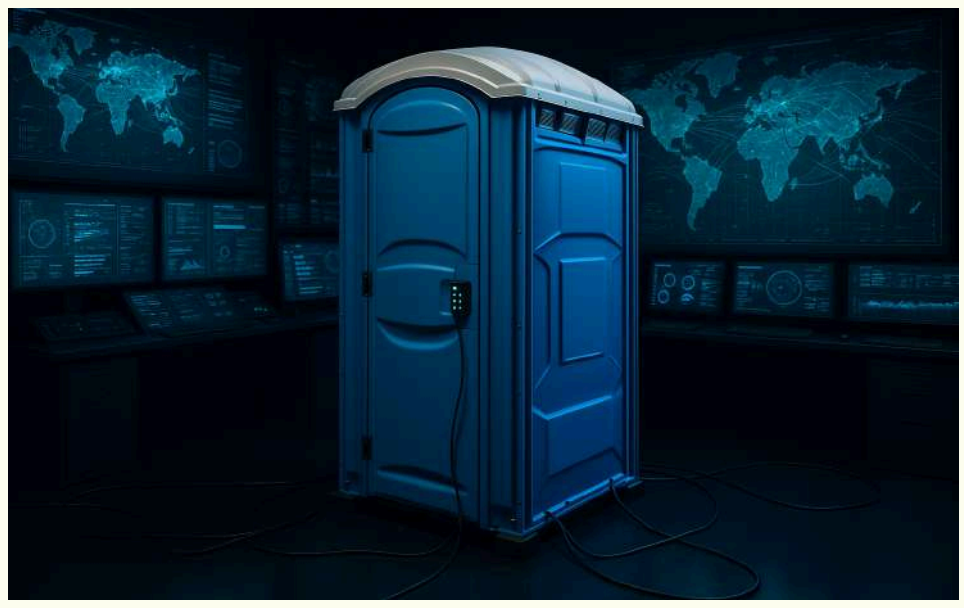


CyAN Cybersecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

40. Unraveling Digital Sovereignty: The Delicate Balance of Digital Sovereignty: Insights and Imperatives

By CyAN Global VP Kim Chandler McDonald



Kim explores the evolving concept of digital sovereignty, urging policymakers to rethink what national control over data truly means in an interconnected world.

Rather than retreating behind digital borders, she advocates for a balanced approach that champions interoperability, individual rights, and shared accountability.

This means designing systems and policies that respect jurisdictional differences while enabling secure, seamless collaboration across borders. It’s about protecting people and principles, not erecting digital walls.

Drawing on recent global trends, Kim calls for collaborative frameworks that support privacy, innovation, and trust—without stifling the cross-border flows that power our digital lives. It’s a timely call to action for those shaping tomorrow’s data governance.

CyAN CyAN Members Op Eds, Articles, etc

"***You have to speak the language of your audience. Otherwise, cybersecurity becomes just words, and small businesses simply don't have time for it.***"

During our recent CyAN APAC Sydney Event, hosted by PeopleBank on March 12th, our VP Kim Chandler McDonald highlighted a critical point: engaging small to medium businesses in cybersecurity requires conversations that resonate directly with their everyday experiences.

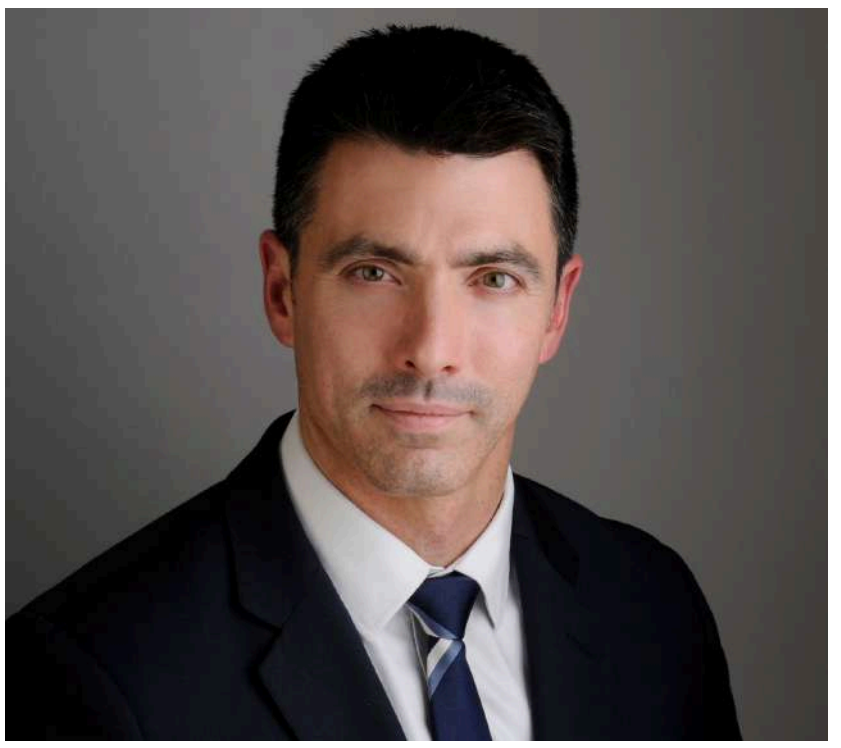
Watch this quick snippet from Kim’s insightful response to an audience question about driving cybersecurity awareness and investment among SMBs.

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!

CyAN member Dan Elliot will be speaking at the Future of Financial Services: Security Sydney on April 1st.



Along with fellow panelists Nathan Lewis, Prakhar Rawat, Ross MacKenzie and will be moderated by Luke Hannan, Dan will be discussing latest advancements in threat intelligence and the ever-evolving threat landscape and how to respond to them.

CyAN member Joe Cozzupoli has been appointed as the Global Ambassador for Australia at the Global Council for Responsible AI. In his new will:

💠 Promote ethical and secure AI practices across Australia and the Asia-Pacific;

💠 Collaborate on global frameworks that ensure transparency, accountability & trust in AI;

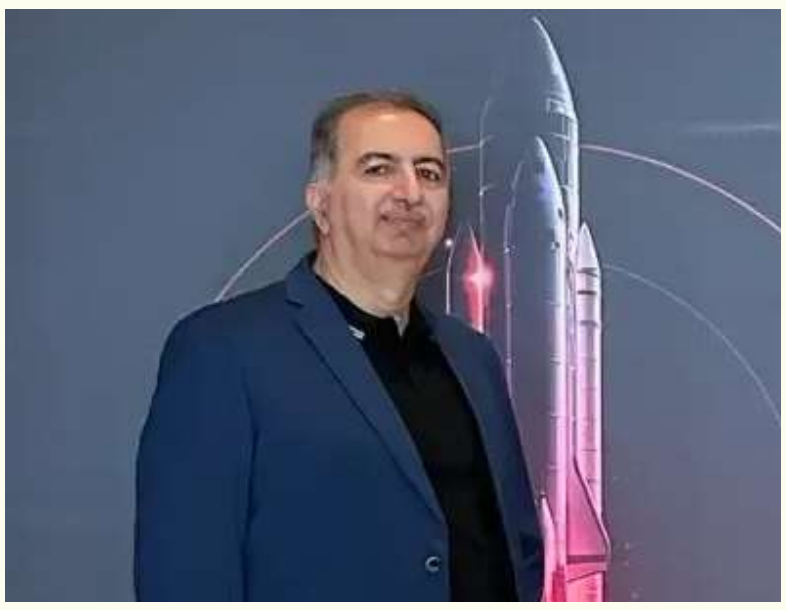
💠 Inspire future leaders and drive innovation through inclusive, values-driven leadership.

Well done Joe!

Supply Chain Cyber Security Summit

9–11 April 2025 | Lisbon, Portugal

Cyan Board Member Bharat is a featured speaker at the Third Party and Supply Chain Cyber Security Summit (SCCS), being held from April 9th to 11th in Lisbon.



Bharat will join over 30 high-level cybersecurity professionals to discuss effective cybersecurity implementation strategies tailored specifically for securing supply chains and third-party partnerships.

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

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