CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #142

NEWS:

1. Ransomware Gangs Innovate With New Affiliate Models

Original Source: Dark Reading by Alexander Culafi

Ransomware groups are evolving fast, experimenting with new affiliate structures that mimic legitimate business models to scale operations and minimise risk. These revised arrangements often include performance-based payouts, decentralised leadership, and pre-packaged “plug-and-play” ransomware kits—making it easier for even low-skilled actors to launch attacks. Researchers warn that this shift is driving an increase in both attack volume and sophistication, blurring the lines between cybercrime syndicates and organised startups. The call to action: treat ransomware as a business—because that’s how they already see it.

CyberSecurity Advisors Network

Anzac Day Publication Change to Schedule

Due to this week's ANZAC Day commemorations and the accompanying long weekend for our editorial team, we'll be adjusting our usual publishing schedule.

There will be just one edition this week, which will go live on Thursday, 24 April.

We appreciate your understanding and look forward to returning to our regular schedule next week.

NEWS:

2. FBI: US lost record $16.6 billion to cybercrime in 2024

Original Source: BleepingComputer by Sergiu Gatlan

The FBI’s latest Internet Crime Report reveals a staggering $16.6 billion in reported cybercrime losses across the U.S. in 2024—a record high and a sharp 22% increase over the previous year. Business email compromise topped the charts once again, followed by investment scams, tech support fraud, and ransomware. The Bureau notes that while reporting is improving, the real numbers may be even higher. Experts say the rise reflects both escalating threat sophistication and continued gaps in organisational defences, urging stronger awareness, incident response, and collaboration at every level.

CyberSecurity Advisors Network

NEWS:

3. Attackers hit security device defects hard in 2024

Original Source: Cyberscoop by Matt Kapko

In 2024, cybercriminals ramped up their exploitation of vulnerabilities in firewalls, VPNs, and other perimeter security devices—tools traditionally seen as a first line of defence. The report highlights how attackers are increasingly targeting zero-days and unpatched flaws in products from major vendors, using them as launching points for deeper intrusions. Experts warn this trend reflects a growing attacker preference for exploiting trusted infrastructure rather than traditional endpoints. Organisations are urged to treat security appliances as potential targets, not just protective layers—and patch accordingly.

CyberSecurity Advisors Network

NEWS:

4. Ripple NPM supply chain attack hunts for private keys

Original Source: The Register by Connor Jones

Developers working with Ripple's XRP ecosystem were targeted in a sophisticated supply chain attack that compromised npm packages to harvest private keys. Attackers injected malicious code into a legitimate-looking package, designed to mimic Ripple's tools, in hopes of stealing credentials from unsuspecting developers. The breach underscores ongoing threats to open-source ecosystems and highlights how attackers are increasingly focusing on upstream software components. Ripple has since responded, but experts warn that dependency hygiene, code reviews, and supply chain monitoring must become standard practice—not optional extras.

CyberSecurity Advisors Network

NEWS:

5. DPRK Hackers Steal $137M from TRON Users in Single-Day Phishing Attack

Original Source: The Hacker News by Ravie Lakshmanan

North Korean threat actors have pulled off a staggering $137 million heist, targeting TRON blockchain users in a single-day phishing campaign. Masquerading as legitimate wallet tools, the attackers tricked users into revealing private keys, enabling swift and large-scale crypto theft. Analysts attribute the attack to a well-coordinated DPRK-backed group known for blending social engineering with technical precision. This incident marks one of the largest TRON-specific thefts to date and highlights the continued vulnerability of decentralised finance platforms to targeted, nation-state-enabled cybercrime.

CyberSecurity Advisors Network

NEWS:

6. Blue Shield of California leaked health data of 4.7 million members to Google

Original Source: BleepingComputer by Bill Toulas

Blue Shield of California has disclosed a data breach affecting 4.7 million members, after inadvertently sharing sensitive health data with Google through tracking technologies embedded in its websites and apps. The exposed data may include medical conditions, treatments, and provider interactions—raising serious HIPAA compliance concerns. While Google claims it didn’t use the data for targeted ads, privacy advocates are sounding the alarm over third-party tracking in healthcare. The breach adds to growing scrutiny of digital health platforms and the urgent need for tighter controls on analytics tools.

CyberSecurity Advisors Network

NEWS:

7.‘Cookie Bite' Entra ID Attack Exposes Microsoft 365

Original Source: Dark Reading by Elizabeth Montalbano

Researchers have uncovered a stealthy new attack dubbed "Cookie Bite" that exploits Entra ID (formerly Azure AD) to gain unauthorised access to Microsoft 365 accounts. By leveraging stolen session cookies and misconfigured identity permissions, attackers can bypass multi-factor authentication and maintain persistence across cloud services. The attack has been observed in the wild and poses a serious threat to organisations relying on Microsoft's cloud ecosystem. Experts urge immediate auditing of identity policies, session management settings, and user permissions to prevent exploitation.

CyberSecurity Advisors Network

NEWS:

8. RIP, Google Privacy Sandbox

Original Source: The Register by Thomas Claburn

Google’s long-touted Privacy Sandbox—meant to replace third-party cookies with a more privacy-conscious ad targeting system—has effectively crumbled under regulatory and industry pressure. The UK’s Competition and Markets Authority has voiced serious concerns, and major stakeholders are pushing back, citing poor transparency and limited control for users. Once pitched as the future of web advertising, the initiative now looks unlikely to deliver on its promises. This collapse signals a broader reckoning for big tech’s attempts to self-regulate privacy while still maintaining advertising dominance.

CyberSecurity Advisors Network

NEWS:

9. Microsoft Purges Millions of Cloud Tenants in Wake of Storm-0558

Original Source: Dark Reading by Jai Vijayan

Following the Storm-0558 espionage campaign, Microsoft has purged millions of inactive Azure AD (now Entra ID) tenants in a sweeping cleanup effort aimed at reducing attack surfaces. The move comes after criticism over lax cloud identity hygiene, which allowed the Chinese threat actor to access sensitive government email accounts. By eliminating dormant tenants—often left misconfigured or forgotten—Microsoft hopes to prevent similar exploits. While applauded by some, the move also raises questions about how such risks went unchecked for so long in one of the world's most widely used cloud environments.

NEWS:

10. Millions of SK Telecom customers are potentially at risk following USIM data compromise

Original Source: Security Affairs by Pierluigi Paganini

SK Telecom, South Korea’s largest mobile operator, is facing scrutiny after reports emerged of a major data breach affecting Universal Subscriber Identity Module (USIM) data. The compromised information—used to authenticate mobile users—could expose millions to SIM swapping, identity theft, and unauthorised access to telecom and banking services. While SK Telecom claims no immediate evidence of abuse, regulators and privacy advocates are demanding transparency and tighter safeguards. The incident highlights growing concerns over mobile infrastructure security and the cascading risks of compromised identity systems.

CyberSecurity Advisors Network

NEWS:

11. Fog ransomware channels Musk with demands for work recaps or a trillion bucks| The Register by Connor Jones

Original Source: The Register by Connor Jones

In a theatrical display of cyber extortion, the Fog ransomware gang is demanding either a trillion-dollar payout or corporate-style work recaps—directly parodying Elon Musk's management emails at X. Victims are greeted with ransom notes that mock internal performance reviews, blending satire with coercion. While the tone may seem absurd, the malware's impact is serious: files are encrypted, systems disrupted, and threats of data leaks loom large. Experts caution that such antics are more than marketing—they're a calculated move to exploit culture, buy time, and throw victims off balance.

CyberSecurity Advisors Network

NEWS:

12. Docker Malware Exploits Teneo Web3 Node to Earn Crypto via Fake Heartbeat Signals

Original Source: The Hacker News by Ravie Lakshmanan

A new malware campaign targeting Docker environments is abusing Teneo Web3 infrastructure to mine cryptocurrency by spoofing node “heartbeat” signals. Once deployed in misconfigured containers, the malware fakes activity signals to extract token-based rewards—draining system resources and enabling persistent abuse. The attack reflects a growing trend of targeting decentralised platforms and developer tools to exploit cloud-native environments. Security experts warn that with Web3 integration accelerating, organisations must secure their DevOps pipelines and closely monitor container behaviour for unusual traffic and resource use.

CyberSecurity Advisors Network

NEWS:

13. Ripple's recommended XRP library xrpl.js hacked to steal wallets

Original Source: BleepingComputer by Lawrence Abrams

Developers using Ripple’s recommended JavaScript library, xrpl.js, are being urged to update immediately after attackers compromised the package to steal users’ XRP wallet credentials. The malicious version was available for several days and designed to harvest secret keys, putting funds at risk across applications that unknowingly integrated the tainted code. Ripple has confirmed the breach and is coordinating with npm to contain the damage. This incident highlights ongoing threats in open-source supply chains and the urgent need for dependency verification, especially in crypto-related development environments.

CyberSecurity Advisors Network

NEWS:

14. DeepSeek Breach Opens Floodgates to Dark Web

Original Source: Dark Reading by Emma Zaballos

A breach at AI firm DeepSeek has reportedly led to a flood of sensitive data being traded on dark web forums, sparking fresh concerns over AI system security and vendor transparency. Attackers claim to have accessed internal logs, training datasets, and user information—though the full extent is still under investigation. The incident raises alarms about the security posture of emerging AI companies handling vast amounts of sensitive input. Experts are calling for tighter controls around AI infrastructure, including stronger access restrictions, better segmentation, and rigorous breach disclosure practices.

NEWS:

15. SuperCard X Android Malware Enables Contactless ATM and PoS Fraud via NFC Relay Attacks

Original Source: The Hacker News by Ravie Lakshmanan

Researchers have uncovered SuperCard X, a sophisticated Android malware that enables contactless fraud by abusing NFC relay attacks. Once installed, it allows cybercriminals to use a victim's payment credentials—often stolen through other malware or phishing—to interact with ATMs and point-of-sale systems without physical access to the card. This attack method circumvents traditional proximity checks, making it nearly impossible for users to detect. The malware underscores growing concerns over mobile payment security and highlights the need for stronger device-level protections and transaction monitoring.

CyberSecurity Advisors Network

NEWS:

16. Billion-dollar cyberscam industry spreading globally, warns UN

Original Source: itNews

A UN report warns that organised cyberscams are ballooning into a billion-dollar global industry, exploiting victims through fraudulent investment schemes, phishing, and forced labour operations in scam centres. Fuelled by geopolitical instability and weak enforcement in certain regions, these scams are increasingly operated by transnational criminal networks using coercion, trafficking, and digital deception to profit at scale. The report urges global cooperation, improved legal frameworks, and greater public awareness to counter this growing threat, which blurs the line between cybercrime and human rights abuse.

NEWS:

17. Researchers warn of critical flaw found in Erlang OTP SSH

Original Source: Cybersecurity Dive by David Jones |

Security researchers have discovered a critical vulnerability in the Erlang/OTP Secure Shell (SSH) implementation, which could allow attackers to bypass authentication and execute arbitrary commands on affected systems. Widely used in telecoms, messaging apps, and IoT environments, Erlang's presence in high-availability systems makes this flaw particularly alarming. The vulnerability stems from incorrect handling of SSH handshake data and has been assigned the highest severity rating. Experts urge immediate patching, warning that exploitation could lead to remote code execution or compromise of critical infrastructure if left unaddressed.

CyberSecurity Advisors Network

NEWS:

18. The FBI Can't Find ‘Missing’ Records of Its Hacking Tools

Original Source: 404 Media by Joseph Cox

The FBI has admitted it cannot locate key internal records related to its use and handling of hacking tools, raising serious concerns about transparency and oversight. The missing documentation pertains to software vulnerabilities and surveillance tools deployed in criminal investigations. Critics argue this gap undermines accountability and complicates efforts to evaluate whether the agency complies with legal and ethical standards. The disclosure, revealed through a FOIA lawsuit, highlights ongoing tensions between national security operations and public demand for transparency in government surveillance practices.

CyberSecurity Advisors Network

NEWS:

19. Microsoft rated this bug as low exploitability. Miscreants weaponized it in just 8 days

Original Source: The Register by Iain Thomson

A security bug that Microsoft initially classified as low-risk was weaponised by threat actors in just eight days, highlighting how quickly underestimated vulnerabilities can escalate. Tracked as CVE-2024-21412, the flaw allowed attackers to bypass Windows Defender SmartScreen protections and deliver malicious payloads with little user interaction. Researchers warn that this incident demonstrates the dangers of relying too heavily on severity scores alone. It also reinforces the need for organisations to monitor exploit trends closely and apply patches proactively—even for issues deemed “low priority.”

CyberSecurity Advisors Network

NEWS:

20. Multiple top CISA officials behind ‘Secure by Design’ resign | Cyberscoop by Derek B. Johnson

Original Source: Cyberscoop by Derek B. Johnson

Several senior officials behind CISA’s flagship “Secure by Design” initiative have unexpectedly resigned, sparking concern over the future direction of the agency’s software security agenda. The departures include key figures who had been pushing for systemic change in how software is built, marketed, and secured across industries. While CISA insists the initiative will continue, the exits raise questions about internal challenges and whether industry momentum around security-by-default principles might stall. With escalating threats and supply chain risks, the timing of this leadership shift could not be more critical.

CyberSecurity Advisors Network

NEWS:

21. North Korean Cryptocurrency Thieves Caught Hijacking Zoom ‘Remote Control’ Feature

Original Source: SecurityWeek by Ryan Naraine

North Korean threat actors have been caught exploiting Zoom’s “Remote Control” feature to hijack user sessions and steal cryptocurrency. By tricking victims into granting control during meetings, attackers gained access to wallets and sensitive data without deploying traditional malware. This social engineering tactic bypasses technical defences by leveraging legitimate functionality, making it harder to detect. Security researchers warn that this marks a shift toward abusing trusted collaboration tools for financial cybercrime, and urge users to be cautious about granting remote access —even within familiar platforms.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

22. Phishers abuse Google OAuth to spoof Google in DKIM replay attack

Original Source: Ionut Ilascu

Cybercriminals are exploiting Google OAuth and DKIM replay tactics to send phishing emails that appear to be genuinely from Google. By replaying previously authenticated messages, attackers bypass email security filters and trick recipients into clicking malicious links or handing over credentials. The abuse of legitimate Google infrastructure gives these phishing attempts an alarming level of credibility. Experts warn that traditional indicators of email authenticity, like DKIM and SPF, can no longer be trusted in isolation. Organisations are urged to adopt multi-layered email security and train staff to spot social engineering tactics.

CyberSecurity Advisors Network

NEWS:

23. Countries Shore Up Their Digital Defenses as Global Tensions Raise the Threat of Cyberwarfare

Original Source: SecurityWeek / Associated Press

As geopolitical tensions surge, nations are racing to fortify their digital infrastructure against the rising threat of cyberwarfare. From Europe to Southeast Asia, governments are investing heavily in critical system resilience, threat intelligence sharing, and cyber-specific military capabilities. Officials warn that attacks on power grids, health systems, and communication networks are no longer hypothetical. Recent incidents have prompted a sense of urgency, with leaders stressing that future conflicts will unfold not just on land, sea, and air—but in the invisible, volatile theatre of cyberspace.

CyberSecurity Advisors Network

NEWS:

24. Hackers Abuse Russian Bulletproof Host Proton66 for Global Attacks and Malware Delivery

Original Source: The Hacker News by Ravie Lakshmanan

Proton66, a Russian bulletproof hosting service, is being exploited by cybercriminals to launch global malware campaigns and host phishing infrastructure. Known for ignoring takedown requests and shielding malicious actors, Proton66 enables attackers to deliver info-stealers, remote access trojans, and ransomware with minimal disruption. Researchers have linked recent attacks across Europe and North America to servers hosted by the service. The report highlights the enduring role of rogue infrastructure providers in sustaining the cybercrime economy and calls for stronger international cooperation to dismantle these digital safe havens.

CyberSecurity Advisors Network

NEWS:

25. FOG Ransomware Spread by Cybercriminals Claiming Ties to DOGE

Original Source: Trend Micro by Nathaniel Morales & Sarah Pearl Camiling

A new ransomware strain dubbed FOG is being distributed by a group claiming affiliation with the pro-privacy DOGE project, though no formal links have been verified. The malware encrypts victim systems and demands payment in cryptocurrency, using DOGE branding to lend credibility and confuse targets. Analysts note the attackers are employing phishing emails, fake updates, and cracked software to spread infections. The campaign underscores the ongoing abuse of decentralised tech communities' reputations to mask criminal intent and highlights the growing use of branding tactics in ransomware operations.

CyberSecurity Advisors Network

NEWS:

26. APT29 Deploys GRAPELOADER Malware Targeting European Diplomats Through Wine-Tasting Lures

Original Source: The Hacker News by Ravie Lakshmanan

APT29, a Russian state-linked threat actor, has been observed targeting European diplomats using a campaign themed around wine-tasting events to deliver new malware dubbed GRAPELOADER. Masquerading as legitimate invitations, the lures trick victims into launching malicious payloads designed for stealthy surveillance and data exfiltration. The campaign exemplifies APT29's blend of tailored social engineering and technical sophistication. Analysts warn that diplomacy remains a prime cyber espionage target, and this creative ruse reinforces the need for heightened awareness and robust phishing defences in sensitive government sectors.

CyberSecurity Advisors Network

NEWS:

27. New Android malware steals your credit cards for NFC relay attacks

Original Source: BleepingComputer by Bill Toulas

A newly discovered Android malware variant is targeting users' credit card data to facilitate near-field communication (NFC) relay attacks. Once installed, the malware harvests payment credentials and enables attackers to perform unauthorised contactless transactions at ATMs and point-of-sale terminals—without needing the physical card. This tactic mirrors the behaviour of SuperCard X, showing a troubling trend toward mobile-based fraud tools capable of bypassing traditional proximity checks. Experts warn users to avoid sideloading apps, keep device security settings locked down, and use strong mobile protection to defend against these increasingly sophisticated threats.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

28. Rogue npm Packages Mimic Telegram Bot API to Plant SSH Backdoors on Linux Systems

Original Source: The Hacker News by Ravie Lakshmanan

Security researchers have uncovered rogue npm packages that impersonate the Telegram Bot API to stealthily install SSH backdoors on Linux systems. These malicious packages were designed to blend into legitimate development workflows, allowing attackers to gain persistent remote access once deployed. The discovery highlights ongoing threats in the software supply chain, particularly in open-source ecosystems where trust in package names and downloads remains high. Developers are urged to scrutinise dependencies, validate package authenticity, and monitor for unusual SSH activity to mitigate risks from such hidden threats.

CyberSecurity Advisors Network

NEWS:

29. Hacking US crosswalks to talk like Zuck is as easy as 1234| The Register by Iain Thomson

Original Source: The Register by Iain Thomson

In a bizarre yet troubling discovery, researchers found that many U.S. pedestrian crosswalk systems are secured with default PINs like “1234,” allowing attackers to hijack the devices and upload custom audio—yes, even Mark Zuckerberg and Elon Musk impressions. These smart crosswalks, intended to aid accessibility, can be wirelessly reprogrammed with minimal effort due to weak authentication practices. While seemingly humorous, the flaw reflects a broader issue: critical public infrastructure is being deployed with poor security hygiene. Experts urge immediate updates to authentication protocols before a prank turns into a more serious safety concern.

CyberSecurity Advisors Network

ANALYSIS:

30. The Foundations of a Resilient Cyber Workforce

Original Source: Dark Reading by Mohan Loo

Building a truly resilient cyber workforce requires more than technical training—it demands a cultural shift. This analysis explores how organisations can foster adaptability, collaboration, and critical thinking within their teams to respond effectively to fast-evolving threats. Rather than focusing solely on recruitment, the piece advocates for ongoing learning, cross-functional communication, and leadership that prioritises psychological safety and mission clarity. With burnout and talent shortages on the rise, resilience is no longer optional—it's a strategic imperative that must be embedded into every layer of the cybersecurity function.

CyberSecurity Advisors Network

ANALYSIS:

31. Nation-State Threats Put SMBs in Their Sights

Original Source: Dark Reading by Robert Lemos

Small and midsize businesses (SMBs) are increasingly finding themselves in the crosshairs of nation-state cyber attackers—not because of what they hold, but because of who they're connected to. As supply chain dependencies grow, state-backed actors are targeting SMBs as stepping stones to larger, better-defended organisations. Despite limited budgets and smaller attack surfaces, these businesses often lack robust defences, making them ideal entry points. The article calls for SMBs to adopt threat modelling that reflects their real-world risk—not just their size—and for national strategies to include them in broader cyber resilience efforts.
[For more on this subject see article number 36 'The Elephant in the Server Room: Why Nation-State Hackers Love Small Businesses']

CyberSecurity Advisors Network

ANALYSIS:

32. Why AI Cyber Defences Are Lagging Behind the Offence

Original Source: PrivID (Substack)

While AI is being rapidly adopted in cybersecurity, defensive applications are struggling to keep pace with offensive innovation. This analysis argues that while attackers use AI to scale and personalise attacks—from phishing to malware generation—defenders remain bogged down by rigid tools, data limitations, and compliance hurdles. The piece calls for more agile, adversarial approaches to AI defence—built on continuous learning, contextual awareness, and human oversight. Without a shift in mindset and architecture, defenders risk falling further behind in a fight that's increasingly automated, adaptive, and asymmetric.

CyberSecurity Advisors Network

ANALYSIS:

33. Can Cybersecurity Weather the Current Economic Chaos

Original Source:Dark Reading by Robert Lemos

With global markets wobbling and budgets tightening, cybersecurity teams are under growing pressure to do more with less. This piece explores how economic instability is affecting staffing, spending, and strategic decision-making across the security sector. While some organisations are trimming investments, others view cybersecurity as a non-negotiable line of defence amid uncertainty. Experts caution against short-term cost-cutting that could lead to long-term risk, especially as threat actors—many of them well-funded—continue to scale up their operations. Resilience, the article argues, requires not just tools, but prioritisation, creativity, and leadership buy-in.

CyberSecurity Advisors Network

ANALYSIS:

34. Bot Traffic Surpasses Humans Online—Driven by AI and Criminal Innovation

Original Source: SecurityWeek by Kevin Townsend

For the first time, bots now account for the majority of internet traffic—with malicious bots representing a record high. Fuelled by advances in AI and the rise of “as-a-service” cybercrime tools, these bots scrape data, commit fraud, and launch attacks at a scale humans simply can’t match. The article explores how automation is tipping the balance online, challenging everything from ad integrity to website performance and cybersecurity norms. Experts call for smarter bot management strategies, warning that without coordinated defences, the internet could become an increasingly hostile, inhuman place.

CyberSecurity Advisors Network

ANALYSIS:

35. 5 Reasons Device Management Isn't Device Trust

Original Source: The Hacker News

For the first time, bots now account for the majority of internet traffic—with malicious bots representing a record high. Fuelled by advances in AI and the rise of “as-a-service” cybercrime tools, these bots scrape data, commit fraud, and launch attacks at a scale humans simply can’t match. The article explores how automation is tipping the balance online, challenging everything from ad integrity to website performance and cybersecurity norms. Experts call for smarter bot management strategies, warning that without coordinated defences, the internet could become an increasingly hostile, inhuman place.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

36. The Elephant in the Server Room: Why Nation-State Hackers Love Small Businesses

By CyAN Global VP Kim Chandler McDonald

In this timely and provocative op-ed, CyAN Global VP Kim Chandler McDonald calls out a blind spot in cybersecurity strategy: the vulnerability of small businesses to nation-state actors.

These attackers aren't just hitting governments or big tech—they're targeting SMBs as soft access points into broader networks. Kim argues this isn't incidental—it's tactical. With limited resources and low defences, small businesses are too often overlooked, leaving critical gaps. She urges decision-makers to shift perspective and treat SMBs not as cyber afterthoughts, but as frontline players in national security and digital resilience.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

37. CyAN's Position on Germany's 2025 Coalition Agreement

By CyAN

CyAN outlines its position on Germany's 2025 Coalition Agreement, highlighting both the opportunities and omissions that will shape the nation's digital future.

While applauding the renewed focus on cybersecurity, data sovereignty, and digital education, CyAN urges greater attention to secure-by-design principles, international collaboration, and support for SMEs. The position paper reflects CyAN's broader mission to influence policy that is technically sound, globally minded, and socially inclusive—ensuring cybersecurity isn't just a national priority, but a shared global responsibility.

CyberSecurity Advisors Network

38. Fortune 500 CEOs on Cybersecurity (2019-2024)

By CyAN member Nick Kelly

CyAN member Nick Kelly presents a compelling longitudinal analysis of how cybersecurity has evolved from a back-office concern to a boardroom priority among Fortune 500 CEOs

By examining five years of CEO commentary and public filings, he highlights shifting attitudes toward cyber risk, governance, and accountability. The report tracks trends like the growing focus on resilience, board-level engagement, and the integration of cyber into business strategy. It also reveals how some industries remain dangerously behind the curve. Nick's insights offer a rare window into executive mindset—valuable for CISOs, advisors, and policymakers alike.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

39. La Liga: Blocking of Cloudflare IPs in Spain

By CyAN Communications Director John Salomon

In this sharp and timely op-ed, CyAN Board Member John Salomon explores the implications of Spain's decision to block Cloudflare IPs in an effort to curb unauthorised sports streaming.

While aimed at piracy, the sweeping move caused widespread collateral damage—disrupting unrelated services and raising serious concerns about internet governance and proportionality. Salomon unpacks the legal, technical, and ethical dimensions of the case, arguing that blunt-force measures like IP blocking risk undermining legitimate services and setting dangerous precedents for digital rights and infrastructure management.

CyberSecurity Advisors Network

CyAN Member's News:

CyAN thrives because of the incredible talent, leadership, and dedication of our members, and we are proud to see them shaping the future of cybersecurity on a global stage! 🚀💙

The International TPRM Alliance kicks off 2025 with the 11th Virtual Summit on April 26. CyAN Board Member Bharat Raigangar will speak on aligning third-party risk with board expectations, while CyAN member Yedhu Krishna Menon serves as Orchestrator and Moderator.

Congrats to both for leading global conversations in risk and governance!

UPCOMING CyAN and CyAN Partner EVENTS:

- 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