CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #109

NEWS:

1. Australia's first Cyber Security Act becomes law

Original Source: ACS Information Age by By Leonard Bernardone

Australia’s inaugural Cyber Security Act has officially passed, mandating critical infrastructure providers to adopt stringent cybersecurity measures.

The legislation focuses on protecting essential services like energy, health, and communications from evolving cyber threats. Businesses are now required to report incidents promptly and meet compliance standards to mitigate risks.

Experts view this as a crucial step in bolstering national resilience, although questions remain about enforcement and SME support.

CyberSecurity Advisors Network

NEWS:

2. China has utterly pwned 'thousands and thousands' of devices at US telcos

Original Source: The Register by Simon

Chinese state-backed hackers have reportedly infiltrated thousands of devices within US telecom networks, exploiting undisclosed vulnerabilities.

The attacks, described as widespread and sophisticated, highlight persistent risks to critical infrastructure. Experts warn that the scale of these breaches demonstrates the need for enhanced supply chain security, stricter vendor vetting, and coordinated responses to state-sponsored cyber threats.

Such incidents underscore ongoing geopolitical tensions in the cyber domain.

CyberSecurity Advisors Network

NEWS:

3. Fancy Bear 'Nearest Neighbor' Attack Uses Nearby Wi-Fi Network

Original Source: Dark Reading by Elizabeth Montalbano

The Russian APT group Fancy Bear has developed a "Nearest Neighbor" attack leveraging unsecured nearby Wi-Fi networks to compromise targets.

This technique allows hackers to infiltrate systems without needing direct network access, posing significant risks to organisations relying on wireless security. The attack highlights vulnerabilities in urban environments, where proximity to targets is easily exploited.

Cybersecurity professionals are urged to review wireless protocols and enhance network segmentation to counter such threats.

CyberSecurity Advisors Network

NEWS:

4. Russian Cyberspies Hacked Building Across Street From Target for Wi-Fi Attack

Original Source: Security Week by Edward Kovacs

Russian cyber-espionage agents reportedly hacked a building across the street from a US company to carry out a Wi-Fi-based cyberattack.

Dubbed the "Nearest Neighbor" attack, this method highlights the lengths state-backed actors will go to infiltrate systems. By exploiting unsecured Wi-Fi networks, attackers bypass traditional defences.

Experts recommend implementing stringent access controls and regular audits of wireless security to reduce risks from close-proximity threats in densely populated areas.

CyberSecurity Advisors Network

NEWS:

5. Bangkok busts SMS Blaster sending 1 million scam texts from a van

Original Source: BleepingComputer by Bill Toulas

Thai authorities have uncovered a mobile SMS-blasting operation sending over a million scam texts from a single van.

The setup, equipped with SIM banks and custom devices, highlights the persistent threat of phishing scams targeting mobile users. Officials are cracking down on these operations, but experts stress the need for public awareness campaigns and telecom cooperation to curb such large-scale fraud.

This case underscores the evolving tactics of cybercriminals exploiting mobile vulnerabilities.

CyberSecurity Advisors Network

NEWS:

6. Salt Typhoon hackers backdoor telcos with new GhostSpider malware

Original Source: BleepingComputer by Bill Toulas

The Salt Typhoon APT group has been deploying GhostSpider malware to infiltrate global telecom networks.

By exploiting vulnerabilities and ‘backdooring’ systems, the group gains access to sensitive communications and operational data. This advanced malware highlights the increasing sophistication of state-sponsored actors targeting critical infrastructure.

Security experts urge telecom providers to prioritise patch management, enhance threat monitoring, and employ advanced endpoint protection to mitigate such risks.

CyberSecurity Advisors Network

NEWS:

7. Australian government dumps plan to regulate online misinformation

Original Source: itNews

Australia has shelved its proposal to regulate online misinformation following backlash from industry groups and civil society. Critics argued the plan could stifle free speech and create compliance burdens for tech platforms.

While the government has pledged to revisit the issue, experts warn that unchecked misinformation continues to pose risks to democratic processes and public trust.

Policymakers must now balance free expression with accountability in addressing digital disinformation.

CyberSecurity Advisors Network

NEWS:

8. North Korean Hackers Steal $10M with AI-Driven Scams and Malware on LinkedIn

Original Source: The Hacker News by Ravie Lakshmanan

North Korean cybercriminals have stolen over $10 million through AI-driven scams and malware distributed via LinkedIn. The attackers use fake profiles and tailored phishing techniques to target victims, blending social engineering with advanced tools to bypass defences.

This incident highlights the growing use of AI in cybercrime and the risks posed by trusted platforms.

Experts recommend vigilance, multi-factor authentication, and employee training to reduce exposure to such sophisticated threats.

CyberSecurity Advisors Network

NEWS:

9. Volunteer DEF CON hackers dive into America's leaky water infrastructure

Original Source: The Register by Iain Thomson

DEF CON volunteers are working to address cybersecurity gaps in America’s water infrastructure, following warnings of potential risks to public safety.

The project has identified outdated systems, weak access controls, and insufficient monitoring as key vulnerabilities. Experts stress the urgent need for investment in modernising critical infrastructure to protect against escalating cyber threats.

This collaboration underscores the role of the cybersecurity community in safeguarding essential services.

CyberSecurity Advisors Network

NEWS:

10. Passwords are giving way to better security methods – until those are hacked too, that is

Original Source: The Guardian by Gene Marks

With passwords increasingly seen as weak points, alternative methods like biometric authentication and passkeys are gaining traction.

However, experts warn that these newer technologies are not immune to hacking and must be paired with robust security frameworks. The shift highlights the need for constant innovation in authentication technologies to outpace evolving threats.

Organisations are urged to adopt a layered approach to security, combining advanced tools with strong user awareness initiatives.

CyberSecurity Advisors Network

NEWS:

11. DOJ seized credit card marketplace PopeyTools and charges its administrators

Original Source: Security Affairs by Pierluigi Paganini

The US Department of Justice has taken down the PopeyTools credit card marketplace, seizing its infrastructure and filing charges against its administrators. PopeyTools facilitated the sale of stolen credit card data, enabling large-scale fraud.

This takedown highlights the importance of international cooperation in dismantling cybercrime networks. Experts stress the need for ongoing efforts to disrupt underground marketplaces and strengthen global financial cybersecurity.

CyberSecurity Advisors Network

NEWS:

12. AI increasingly used for sextortion, scams and child abuse, says senior UK police chief

Original Source: The Observer by Lizzie Dearden

A senior UK police official has warned about the alarming rise of AI in enabling sextortion, financial scams, and child exploitation.

Deepfake technology and AI-generated content are being weaponised to deceive and manipulate victims, complicating law enforcement efforts.

Authorities are calling for stricter AI regulations and enhanced public awareness to combat these emerging threats.

Experts stress that collaboration between policymakers, tech companies, and law enforcement is critical to tackling this growing misuse of AI.

CyberSecurity Advisors Network

NEWS:

13. Hackers abuse Avast anti-rootkit driver to disable defenses

Original Source: BleepingComputer by Bill Toulas

Cybercriminals have exploited a vulnerability in Avast's anti-rootkit driver to disable endpoint defences and escalate attacks.

The abuse of legitimate software underscores the evolving tactics of attackers using trusted tools to bypass detection.

Avast has issued updates to address the flaw, and experts recommend organisations regularly update software and deploy endpoint detection solutions to mitigate risks.

This incident highlights the importance of monitoring for misuse of legitimate software in cybersecurity strategies.

CyberSecurity Advisors Network

NEWS:

14. Andrew Tate's site ransacked, subscriber data stolen

Original Source: The Register by Iain Thomson

Hackers have breached Andrew Tate’s website, exfiltrating sensitive subscriber data, including personal information and payment details.

The incident raises concerns about the security practices of high-profile individuals and their platforms. Experts recommend robust security measures, such as regular penetration testing and multi-factor authentication, to safeguard personal brands and online communities.

This breach underscores the growing risk of cyberattacks targeting celebrity-run digital assets.

CyberSecurity Advisors Network

NEWS:

15. Faux ChatGPT, Claude API Packages Deliver JarkaStealer

Original Source: Dark Reading by Nate Nelson

Malicious packages masquerading as ChatGPT and Claude APIs are delivering the JarkaStealer malware, targeting developers and organisations.

Distributed via compromised software repositories, the malware exfiltrates sensitive data, including login credentials and API keys.

This highlights the risks of supply chain attacks in software development environments. Experts urge developers to verify the integrity of third-party packages and adopt security tools to detect malicious dependencies in codebases.

CyberSecurity Advisors Network

NEWS:

16. 1,000s of Palo Alto Networks firewalls hijacked as miscreants exploit critical hole

Original Source: The Register by Jessica Lyons

Over 1,000 Palo Alto Networks firewalls have been compromised as attackers exploit a recently patched vulnerability, highlighting the risks of delayed updates.

These breaches allow unauthorised access to critical systems, jeopardising sensitive data and operations. Experts emphasise the importance of timely patch management and advanced monitoring to detect unusual activity.

Organisations are urged to prioritise proactive defense strategies to protect critical infrastructure from similar exploits.

CyberSecurity Advisors Network

NEWS:

17. Stronger cyber protections in health care targeted in new Senate bill

Original Source: CyberSnoop by Matt Bracken

A newly introduced US Senate bill aims to strengthen cybersecurity in the healthcare sector, focusing on critical vulnerabilities that put patient data and services at risk.

The proposed legislation includes measures to improve incident reporting, enhance collaboration, and fund modernised defences for healthcare providers.

Lawmakers are responding to increasing attacks on hospitals and medical systems, emphasising the need for proactive measures to safeguard patient safety and sensitive information.

CyberSecurity Advisors Network

NEWS:

18. Leaky Cybersecurity Holes Put Water Systems at Risk

Original Source: Dark Reading by Robert Lemos

Critical water infrastructure remains vulnerable to cyberattacks due to outdated systems and insufficient cybersecurity measures, leaving essential services exposed to disruption.

Experts warn that weak access controls and unpatched vulnerabilities create significant risks to public safety.

Recent analyses call for urgent investment in upgrading water system defences, implementing real-time monitoring, and enhancing incident response capabilities to prevent catastrophic failures in critical infrastructure.

CyberSecurity Advisors Network

NEWS:

19. Wire cutters: how the world's vital undersea data cables are being targeted

Original Source: The Guardian by Dan Milmo

Undersea data cables, which facilitate global internet connectivity, are increasingly at risk from targeted attacks and geopolitical tensions.

These cables are critical to economic and communication stability, yet they remain poorly protected against sabotage.

Experts are urging nations to enhance surveillance and build redundancies to safeguard this infrastructure.

The rising threat to subsea cables highlights the need for international cooperation to address vulnerabilities in this essential network.

CyberSecurity Advisors Network

NEWS:

20. Quishing’, ‘vishing’ and AI scams – the new cybercriminal techniques duping Australians

Original Source: The Guardian by Josh Butler

Cybercriminals are evolving their tactics with methods like “quishing” (QR code phishing), “vishing” (voice phishing), and AI-driven scams.

Australians are increasingly targeted by these sophisticated schemes, which exploit trust and new technologies to steal data or funds.

Experts recommend public awareness campaigns, multi-factor authentication, and robust endpoint protections to counter these emerging threats.

As cybercriminal methods advance, proactive defense and education are critical to staying ahead.

CyberSecurity Advisors Network

NEWS:

21. Social media ban bill lifts online safety fines to $50m

Original Source: InnnovationAus by Justin Hendry

A proposed Australian bill targeting online safety introduces fines of up to $50 million for social media platforms that fail to comply with new safety standards.

The legislation aims to address harmful content, improve reporting mechanisms, and enforce accountability on tech companies.

Critics argue that the penalties may be difficult to enforce, but proponents view this as a necessary step to protect users, particularly children, from online abuse and exploitation. The debate underscores the balance between safety and regulation.

CyberSecurity Advisors Network

ANALYSIS:

22. Banning under-16s from social media ripe for High Court challenge

Original Source: InnovationAus by Sarah Joseph

A proposed law banning under-16s from social media in Australia is facing criticism and potential legal challenges over concerns it infringes on personal freedoms and parental rights.

The policy aims to protect minors from harmful content but raises questions about enforcement and the broader implications for digital access.

Experts warn that implementing such a ban could face significant hurdles in the High Court, with some advocating for improved safety features over outright restrictions.

CyberSecurity Advisors Network

ANALYSIS:

23. Trump taps border hawk to head DHS. Will Noem's 'enthusiasm' extend to digital domain?

Original Source: The Register by Jessica Lyons

South Dakota Governor Kristi Noem, known for her hardline stance on border security, has been tapped by Trump to head the Department of Homeland Security if he is re-elected.

Questions abound over whether her focus will extend to digital threats, given DHS's pivotal role in cybersecurity.

Experts highlight the need for leadership that prioritises both physical and digital resilience, as escalating cyberattacks threaten critical infrastructure and national security.

CyberSecurity Advisors Network

ANALYSIS:

24. A long time coming: Australia's first Cyber Security Bill 2024

Original Source: Norton Rose Fulbright by Annie Haggar

Australia's first Cyber Security Bill has been a milestone in addressing evolving cyber threats.

The legislation introduces mandatory reporting for cyber incidents, alongside a compliance framework for critical infrastructure providers.

Legal experts praise its potential to enhance national security but caution that the implementation may burden smaller businesses.

The bill reflects Australia's commitment to cybersecurity, signalling a shift toward proactive defense measures in the digital age.

CyberSecurity Advisors Network

CyAN MEMBER NEWS:

25. Beyond the Firewall: UAE's Financial Security Evolution

Original Source: Enterprise IT World MEA featuring CyAN's MEA & India Growth Advisor - MEA & India, Bharat Raigangar

CyAN's Bharat Raigangar in discussion with Dr. Mathew Nicho discuss the UAE's innovative approaches to enhancing financial cybersecurity in a rapidly digitising economy and Dr. Nicho's Cyber 'Threat Report: The UAE Financial Sector Cyber Threat Landscape'.

Their conversation highlights key challenges, including the rise of financial crime and the importance of balancing regulation with innovation. They emphasise the need for stronger collaboration between public and private sectors to address evolving threats and safeguard critical financial systems and the UAE's advancements in positioning it as a leader in global financial security.

CyberSecurity Advisors Network

CyAN MEMBER NEWS:

26. 16 Days of Activism Against Gender-Based Violence - Breaking Chains: Standing Against Technology-Facilitated Abuse and Online Violence

Original Source: CyAN Global VP, Kim Chandler McDonald

As part of the global 16 Days of Activism Against Gender-Based Violence, CyAN's Kim Chandler McDonald highlights the urgent need to address technology-facilitated abuse and online violence. From cyberstalking to coercive control, digital platforms are increasingly weaponised against women. This campaign advocates for stronger regulations, better education, and collaboration between tech companies and policymakers to create safer digital spaces. CyAN remains committed to supporting this vital initiative.

CyberSecurity Advisors Network

CyAN NEWS:

27. CyAN Sponsored Awards!

CyAN proudly sponsored two prestigious awards at the recently concluded Supply Chain CyberSecurity Summit, held in Dubai, U.A.E., on November 20–21, 2024: Best TPRM Program and Best Innovative CyberSecurity Solution for Supply Chain.

The Best TPRM Program was awarded to Syed Ubaid Ali Jafri, Head of Cyber Defense & Offensive Security at Habib Bank Limited (HBL). His innovative framework has significantly enhanced HBL's ability to manage third-party risks and serves as a model for effective risk assessment across industries.

The Best Innovative CyberSecurity Solution for Supply Chain went to Finesse for their CyberHUB RiskOpsAI™. This cutting-edge solution exemplifies their commitment to solving complex cybersecurity challenges and building stronger, more resilient supply chains.

A huge congratulations to all the winners for their remarkable achievements!

CyberSecurity Advisors Network

UPCOMING CyAN EVENTS

Sydney: November 27
Women (and their allies!) in Cyber... and a kick off to the festive season!

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