CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #110

ANALYSIS:

1. Labor has passed its proposed social media ban for under-16s. Here's what we know – and what we don't

Original Source: The Guardian by Josh Butler

The newly passed social media ban for under-16s without parental consent has sparked debate about its enforcement and broader implications.

Critics question how age verification will work, particularly the potential need for children to provide ID, raising privacy concerns about how such data will be collected, stored, and used. While the policy aims to shield minors from harmful content and exploitation, concerns persist about excluding young people from valuable educational and social opportunities online.

Advocates argue that it sets a global benchmark for protecting children in digital spaces. This bold move forces Australia to navigate the complex balance between safety, privacy, and digital inclusivity.

CyberSecurity Advisors Network

NEWS:

2. NHS major 'cyber incident' forces hospitals to use pen and paper

Original Source: The Register by Connor Jones

A severe cyberattack has disrupted NHS services, forcing hospitals to revert to manual operations using pen and paper. The incident has significantly slowed medical workflows and impacted patient care, underlining the vulnerabilities in healthcare IT systems.

Experts stress the need for robust cybersecurity measures, including regular patching and incident response planning, to safeguard critical healthcare infrastructure. Investigations are ongoing to determine the attackers' methods and motives. This event highlights the growing threat of ransomware targeting essential public services.

CyberSecurity Advisors Network

NEWS:

3. Beware: AI-Driven Black Friday Scams Are Looming — Here's What to Know

Original Source: eWeek by Sunny Yadav

As Black Friday approaches, cybercriminals are leveraging AI to create convincing scams that target online shoppers. Techniques include fake websites, phishing emails, and AI-generated voice scams designed to steal personal and financial information.

Security experts advise consumers to verify websites, use secure payment methods, and be cautious of deals that appear too good to be true. Retailers are also urged to bolster their defences against potential fraud. Awareness and vigilance remain key to preventing holiday-season cybercrime.

CyberSecurity Advisors Network

NEWS:

4. The only thing worse than being fired is scammers fooling you into thinking you're fired

Original Source: The Register by Jessica Lyons

Cybercriminals are exploiting fears of job insecurity by sending fake termination notices designed to trick employees into revealing sensitive information. These scams prey on emotional responses, leading victims to click on malicious links or download malware.

Security experts recommend verifying such notices through official channels and being cautious of unexpected emails. The rise of this tactic underscores the need for heightened awareness and employee training on phishing threats. Organisations are urged to implement strong email security measures to prevent such attacks.

CyberSecurity Advisors Network

NEWS:

5. Sweden Requests Chinese Bulk Carrier To Stay in Swedish Water as Investigation Into Undersea Fiber-Optic Cables Continues

Original Source: USNI News by John Grady

Swedish authorities have detained a Chinese bulk carrier as part of an investigation into damage to undersea fiber-optic cables.

These cables are critical to global internet connectivity, and their sabotage raises concerns about geopolitical tensions and cyber-physical security. Investigators suspect potential tampering linked to state-backed actors, though evidence remains inconclusive.

This incident highlights the vulnerability of subsea infrastructure to disruption and the need for enhanced monitoring. International cooperation is crucial to safeguarding this vital communication backbone.

CyberSecurity Advisors Network

NEWS:

6. Script Kiddie 'Matrix' Builds Massive Botnet

Original Source: SMG Data Breach Today by Prajeet Nair

A hacker known as "Matrix" has constructed a vast botnet using off-the-shelf tools, demonstrating that even low-skill attackers can create significant disruptions.

The botnet has been used for DDoS attacks and credential theft, exploiting vulnerable IoT devices. Experts emphasise the importance of patching and securing internet-connected devices to prevent such large-scale attacks.

This case underscores how accessible hacking tools have lowered the barrier to entry for cybercriminals. Organisations must prioritise robust defences to mitigate such threats.

CyberSecurity Advisors Network

NEWS:

7. How an AI granny is combating phone scams

Original Source: CNN Business by Hanna Ziady

An AI-powered "granny" chatbot is being used to waste scammers' time and protect potential victims from falling for phone scams. Developed as a decoy, the AI engages fraudsters in lengthy conversations, diverting their resources and reducing their ability to target real victims. T

he project highlights innovative approaches to combating social engineering and telecommunication fraud. While effective, experts warn it’s not a replacement for broader public awareness and systemic regulatory measures.

The initiative demonstrates the creative use of AI for defensive purposes in cybersecurity.

CyberSecurity Advisors Network

NEWS:

8. Starbucks has gone back to pen and paper after vendor ransomware attack

Original Source: TechRadar by Ellen Jennings-Trace

A ransomware attack on a key Starbucks vendor has disrupted digital systems, forcing stores to revert to manual operations. The breach highlights supply chain vulnerabilities and the risks of third-party dependencies in business continuity.

Experts stress the need for robust vendor assessments, incident response plans, and zero-trust architectures to mitigate such risks. Starbucks is working to restore operations while ensuring no customer data was compromised. This incident emphasises the broader impact of ransomware attacks beyond direct victims.

CyberSecurity Advisors Network

NEWS:

9. Data broker leaves 600K+ sensitive files exposed online

Original Source: The Register by Jessica Lyons

A data broker has left over 600,000 sensitive files unsecured on a publicly accessible server, exposing personal information such as names, addresses, and financial records.

The breach highlights the dangers of inadequate data management and the need for stricter regulation of data brokerage firms.

Cybersecurity experts urge businesses to audit their data storage practices regularly and ensure sensitive information is adequately protected. The exposed data poses risks of identity theft and fraud to affected individuals. Regulatory action may be necessary to address industry-wide negligence.

CyberSecurity Advisors Network

NEWS:

10. Romania’s president summons defense council over cyber election interference risk

Original Source: Politico by Carmen Paun

Romania's president has convened a defense council meeting to address growing concerns about cyber threats targeting the country’s upcoming elections.

Officials cite risks of disinformation campaigns, infrastructure sabotage, and digital voter manipulation. This move underscores the increasing geopolitical impact of cyberattacks on democratic processes. Experts recommend enhanced cybersecurity measures, public awareness campaigns, and international collaboration to safeguard electoral integrity.

The situation reflects broader global concerns about cyber threats to elections.

CyberSecurity Advisors Network

NEWS:

11. Victims Must Disclose Ransom Payments Under Australian Law

Original Source: ISMG Info Risk Today by Jayant Chakravarti

Australia’s new legislation mandates that victims of ransomware attacks must report ransom payments to the government within a set timeframe.

The law aims to provide authorities with better data on ransomware trends and disrupt criminal operations. While proponents praise the move as a step toward transparency, critics argue it may deter businesses from reporting incidents altogether.

Experts emphasise the need for supportive frameworks to encourage compliance without penalising victims. The law reflects Australia’s broader effort to combat ransomware effectively.

CyberSecurity Advisors Network

NEWS:

12. Interpol Clamps Down on Cybercrime and Arrests Over 1,000 Suspects in Africa

Original Source: Security Week / Associated Press

Interpol has arrested over 1,000 suspects in a major crackdown on cybercrime operations across Africa. The coordinated effort targeted phishing schemes, financial fraud, and online scams, seizing millions in assets.

Authorities credit international collaboration for the operation's success, highlighting the global nature of cybercrime. Experts stress the importance of continuing such efforts to dismantle criminal networks and build cybersecurity capacity in vulnerable regions.

This marks a significant step in addressing the digital threats facing developing economies.

CyberSecurity Advisors Network

NEWS:

13. Man accused of hilariously bad opsec as alleged cybercrime spree detailed

Original Source: The Register by Connor Jones

A suspected cybercriminal has been arrested following a series of attacks marred by poor operational security (opsec). Authorities discovered key evidence, including incriminating files and personal identifiers, stored in unencrypted formats.

The case underscores the importance of thorough investigative work and highlights how even basic mistakes can lead to the downfall of cybercriminals.

Experts note that while the case is amusing, it reflects broader concerns about the accessibility of hacking tools. Improved public-private cooperation remains critical to combating cybercrime effectively.

CyberSecurity Advisors Network

NEWS:

14. New NachoVPN attack uses rogue VPN servers to install malicious update

Original Source: Bleeping Computer by Sergiu Gatlan

Cybercriminals are exploiting rogue VPN servers under the guise of NachoVPN to distribute malicious updates to unsuspecting users. The malware targets credentials and sensitive data, emphasising the risks of using untrusted VPN providers.

Experts urge businesses and individuals to vet their VPN services carefully and implement strong endpoint protections. This attack highlights the dangers of relying on third-party tools without adequate scrutiny. Users are advised to adopt zero-trust principles for secure network access.

CyberSecurity Advisors Network

NEWS:

15. “RomCom' APT Mounts Zero-Day, Zero-Click Browser Escapes in Firefox, Tor

Original Source: Dark Reading by Nate Nelson

The RomCom APT group has launched sophisticated attacks exploiting zero-day vulnerabilities in Firefox and Tor browsers. These zero-click exploits allow attackers to compromise systems without user interaction, posing significant risks to privacy-focused individuals and organisations.

Experts recommend applying security patches immediately and using layered defences to mitigate potential breaches. This incident underscores the increasing complexity of APT tactics and the importance of proactive threat management.

Organisations must remain vigilant against emerging threats targeting critical applications.

CyberSecurity Advisors Network

NEWS:

16. Medical Specialty Groups: Why Cybercriminals are After Them

Original Source: ISMG Data Break Today by Marianne Kolbasuk McGee

Cybercriminals are increasingly targeting medical specialty groups due to their access to sensitive patient data and limited cybersecurity resources. These groups often lack the infrastructure to defend against sophisticated attacks, making them prime targets for ransomware and data theft.

Experts urge healthcare organisations to adopt stronger encryption, implement zero-trust architectures, and conduct regular security training for staff. The rise in attacks highlights vulnerabilities in niche healthcare sectors.

Greater investment in cybersecurity is essential to protect patient privacy and maintain operational resilience.

CyberSecurity Advisors Network

NEWS:

17. Senators propose law to require bare minimum security standards

Original Source: The Register by Jessica Lyons

US lawmakers have introduced a bill mandating basic cybersecurity standards for all devices connected to the internet. The proposed legislation seeks to close gaps exploited by attackers targeting poorly secured systems, such as IoT devices.

Critics argue the bill doesn't go far enough, while proponents see it as a necessary first step toward broader regulatory reform. Security experts emphasise the importance of public-private collaboration to ensure compliance and effective implementation.

If passed, this could mark a turning point in addressing systemic vulnerabilities.

CyberSecurity Advisors Network

NEWS:

18. Sextortion attacks on the rise and growing in sophistication

Original Source: ITWIRE by Gordon Peters

Sextortion scams are increasing in frequency and complexity, with attackers leveraging social engineering and advanced technologies to exploit victims.

Cybercriminals are using AI-generated content and detailed personal data to lend credibility to their threats. Experts recommend public awareness campaigns, strong privacy practices, and multi-factor authentication to reduce exposure to such scams. Law enforcement agencies are ramping up efforts to combat sextortion, but collaboration with tech platforms is critical.

This trend underscores the need for vigilance against emerging online threats.

CyberSecurity Advisors Network

NEWS:

19. AFP gathers intel after Manila scam ‘boiler room’ raid

Original Source: itNews by Ry Crozier

The Australian Federal Police (AFP) is analysing data seized during a raid on a Manila-based scam operation, known as a "boiler room." The group allegedly targeted Australian victims with fraudulent investment schemes, stealing millions.

This operation highlights the global nature of financial fraud and the importance of cross-border cooperation in tackling cybercrime. Experts stress the need for tighter regulations and improved consumer awareness to mitigate such risks.

The AFP’s investigation is expected to uncover valuable insights into the scammers’ tactics.

CyberSecurity Advisors Network

NEWS:

20. Telco engineer who spied on US employer for Beijing gets four years in the clink

Original Source: The Register Laura Dobberstein

A telecom engineer has been sentenced to four years in prison for spying on their US employer and sharing sensitive information with Chinese authorities.

The case highlights the persistent risks of insider threats, particularly in sectors handling critical infrastructure and national security.
Organisations are urged to strengthen insider threat programs, implement stricter access controls, and monitor for suspicious activity.

This incident underscores the role of human factors in cybersecurity breaches. Governments are calling for increased vigilance against state-sponsored espionage.

CyberSecurity Advisors Network

NEWS:

21. CISA Urges Agencies to Patch Critical "Array Networks" Flaw Amid Active Attacks

Original Source: The Hacker News by Ravie Lakshmanan

The US Cybersecurity and Infrastructure Security Agency (CISA) has issued an urgent directive for federal agencies to patch a critical vulnerability in Array Networks devices.

The flaw is actively being exploited by attackers to gain unauthorised access to sensitive systems. Experts warn that delayed patching could leave critical infrastructure vulnerable to significant breaches.

Organisations are urged to prioritise updates and enhance monitoring to detect potential exploitation. This incident underscores the need for proactive vulnerability management to mitigate risks.

CyberSecurity Advisors Network

NEWS:

22. How the far right is weaponising AI-generated content in Europe

Original Source: The Guardian by Ben Quinn & Dan Milmo

Far-right groups in Europe are increasingly using AI-generated content to amplify disinformation campaigns and influence public opinion.

These tactics include creating deepfake videos, spreading false narratives, and exploiting social media algorithms to reach wider audiences. Experts warn that this trend threatens democratic processes and underscores the need for robust content moderation and regulatory oversight.

Public awareness and digital literacy are critical to countering such manipulation. Governments must also address the ethical implications of AI misuse in political contexts.

CyberSecurity Advisors Network

NEWS:

23. Britain Putin up stronger AI defences to counter growing cyber threats

Original Source: The Register by Iain Thomson

The UK government is ramping up its AI defences to counteract the rising threat of AI-driven cyberattacks. Initiatives include funding for research into AI security, developing national strategies, and enhancing collaboration with international allies.

Experts emphasise the importance of securing AI systems to prevent exploitation by malicious actors. The move reflects growing recognition of AI as both an opportunity and a potential threat in the cybersecurity landscape.

Public and private sectors are urged to work together to build resilient defences against emerging AI-related risks.

CyberSecurity Advisors Network

NEWS:

24. Cyberattacks cost British businesses $55 billion in past five years, broker says

Original Source: Reuters by Carolyn Cohn

A recent report reveals that cyberattacks have cost British businesses an estimated $55 billion over the past five years. These costs include data breaches, ransomware payments, and recovery expenses, with small businesses disproportionately affected.

Experts stress the need for better investment in cybersecurity, particularly for SMEs with limited resources. The findings highlight the economic impact of cybercrime and the importance of adopting proactive measures to mitigate risks.

Collaboration between businesses, insurers, and regulators is essential to strengthen cyber resilience.

CyberSecurity Advisors Network

NEWS:

25. Meta Has Removed Two Million Scam Account This Year

Original Source: Tech.co by Katie Scott

Meta has announced the removal of over two million scam accounts in 2023, targeting fraudulent activities such as phishing, financial scams, and fake advertisements.

The company has enhanced its detection algorithms and partnered with law enforcement to address these threats. While these efforts mark progress, experts warn that scammers are adapting quickly, requiring ongoing vigilance and innovation in platform security.

Users are advised to remain cautious and report suspicious accounts. The scale of this takedown underscores the persistent challenge of combating online fraud.

CyberSecurity Advisors Network

ANALYSIS:

26. Australia introduces Comprehensive Cyber Security Legislation

Original Source: Corrs Chambers Westgarth by CyAN Member Michael do Rozario + James North, Philip Catania & Jack Matthews

Australia has introduced a landmark Cyber Security Act aimed at safeguarding critical infrastructure and mandating incident reporting for cyberattacks.

The legislation sets out compliance obligations for businesses, emphasising accountability, resilience, and robust defences against evolving threats. While experts praise the Act as a step forward in strengthening national cybersecurity, concerns remain about its enforcement and the burden it places on smaller enterprises.

The Act highlights Australia's proactive stance in addressing its digital vulnerabilities. Its implementation is expected to set a global benchmark for cybersecurity governance.

CyberSecurity Advisors Network

ANALYSIS:

27. Closing the Cybersecurity Career Diversity Gap

Original Source: Dark Reading by Theresa Payton

The lack of diversity in the cybersecurity workforce continues to hinder innovation and problem-solving within the industry. Women and underrepresented groups face barriers to entry, including unconscious bias and limited access to mentorship opportunities.

Experts advocate for targeted initiatives, such as scholarships, mentorship programs, and inclusive hiring practices, to close the gap. Increasing diversity is not only an ethical imperative but also a strategic advantage in tackling evolving cyber threats.

Industry leaders are urged to prioritise inclusivity to foster a more dynamic and resilient cybersecurity landscape.

CyberSecurity Advisors Network

NEWS:

28. An opportunity for Trump’s deregulation journey: Cybersecurity harmonization

Original Source: CyberScoop by Brandon Pugh

Former President Trump’s deregulation agenda could extend to cybersecurity harmonisation, emphasising streamlined standards to reduce compliance burdens on businesses. Proponents argue that consolidating regulations could enhance efficiency and foster innovation, while critics warn it may weaken protections.

Harmonisation efforts must balance business interests with the need to safeguard critical systems from escalating cyber threats. Experts call for industry input and collaboration to ensure such reforms achieve meaningful outcomes.

The proposal reflects ongoing debates about the role of regulation in cybersecurity.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

STATISTICS & INSIGHTS
powered by evisec

29. Highlights from last week's cybersecurity research

Original Source: CyAN Member and evisec CEO Henry Röigas

- A paradoxical reality: A survey of 2,800 security professionals shows that 100% are using AI in development, yet they rank "AI-generated code" as their top security concern.
- Security vs speed: 84% say security processes are the main source of delays, while 71% acknowledge that rushed time-to-market pressures still lead to vulnerabilities.
- Shift to managed services: Nearly 20% of companies are cutting hiring budgets, reflecting a growing reliance on Managed Security Services.
- False positives: Practitioners estimate that 34% of threat detection alerts are false positives, exposing inefficiencies in existing tools.

CyberSecurity Advisors Network

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