CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #127

CyAN Cybersecurity Advisors Network

NEWS:

1. Flaw found in stalkerware apps, exposing millions of people. Here's how to find out if your phone is being spied upon

Original Source: Bitdefender by Graham Cluley

A significant security flaw discovered in stalkerware apps has exposed millions to potential spying, significantly compromising user privacy.

This vulnerability allows unauthorised access to personal data, raising serious concerns about the safety and security of individuals who may be unknowingly monitored. The issue highlights the urgent need for users to check their devices for signs of stalkerware, which may include unusual battery drain or data usage.

Experts recommend regular security checks, the installation of reputable anti-stalware tools, and staying informed about the ways to protect personal digital spaces from such invasive software.

CyberSecurity Advisors Network

NEWS:

2. Exploits for unpatched Parallels Desktop flaw give root on Macs

Original Source: BleepingComputer by Bill Toulas

An unpatched vulnerability in Parallels Desktop for Mac allows attackers to gain root access, posing severe risks to users by potentially compromising system integrity and personal data.

This exploit enables unauthorised users to bypass security mechanisms, manipulate systems, and access confidential information, illustrating the critical importance of regular software updates and vigilant security practices.

Mac users are urged to apply all available security patches to mitigate this risk. The situation underscores the necessity of proactive cybersecurity measures and the dangers of operating systems without the latest security defenses.

CyberSecurity Advisors Network

NEWS:

3. DeepSeek's ByteDance Data-Sharing Raises Fresh Security Concerns

Original Source: Dark Reading by Elizabeth Montalbano

Recent reports have raised significant security concerns over DeepSeek, a subsidiary of ByteDance, and its data-sharing practices, which may compromise user privacy.

The scrutiny comes amidst allegations that the company shares user data in ways that could violate privacy norms and potentially aid in surveillance. This issue underscores the need for stringent data governance and highlights the challenges users face in controlling their personal information.

The situation calls for urgent regulatory actions to ensure that data handling by tech companies adheres to ethical standards and legal requirements, protecting individuals from unauthorised data exploitation

CyberSecurity Advisors Network

NEWS:

4. New Malware Campaign Uses Cracked Software to Spread Lumma and ACR Stealer

Original Source: The Hacker News by Ravie Lakshmanan

A new malware campaign exploiting cracked software to spread Lumma and ACR Stealer has been uncovered, targeting users looking for free software alternatives.

This campaign leverages the allure of cracked software to deploy malware that can steal sensitive information, including passwords and financial data. The use of such software poses significant risks, as it often bypasses traditional antivirus protections.

Cybersecurity experts strongly advise against the use of pirated software and emphasise the importance of maintaining rigorous security protocols, including using only legitimate and licensed software, conducting regular system scans, and keeping all software up to date to avoid falling victim to these sophisticated cyber threats.

CyberSecurity Advisors Network

NEWS:

5. Engineers Australia launches ‘chartered’ cyber credential

Original Source: InnovationAus by David McClure

Engineers Australia has introduced a new 'chartered' credential for cybersecurity professionals, aiming to standardise and elevate the expertise within the industry.

This credential is designed to recognise and certify the skills and knowledge of engineers working in the rapidly evolving field of cybersecurity. It offers a structured pathway for professional development, ensuring that practitioners meet the highest standards of competence and ethical practices.

The initiative responds to the increasing complexity of cyber threats and the critical need for qualified professionals who can navigate and secure modern digital infrastructures. The credential not only enhances individual careers but also contributes to the broader goal of fortifying national and organisational cybersecurity capabilities.

CyberSecurity Advisors Network

NEWS:

6. The software UK techies need to protect themselves now Apple's ADP won’t

Original Source: The Register by Connor Jones

With Apple's decision to not extend Advanced Data Protection (ADP) to the UK, tech professionals are urged to explore alternative software solutions to safeguard their digital assets effectively.

This situation highlights the need for robust, end-to-end encryption and other security measures that can compensate for the lack of ADP.

The discussion includes a variety of software options that offer strong encryption standards and data protection policies, aiming to assist UK techies in maintaining their privacy and data integrity against potential cyber threats. The article emphasises the importance of proactive security practices in a landscape where traditional data protection mechanisms are increasingly insufficient.

CyberSecurity Advisors Network

NEWS:

7. Gov bans Kaspersky from its systems and devices

Original Source: itNews by Eleanor Dickinson

The Australian government has implemented a ban on Kaspersky software across all its systems and devices due to security concerns, marking a significant stance on protecting national security.

This precautionary measure addresses the risks associated with potential espionage and cyberattacks that could exploit vulnerabilities within the software.

The ban underscores the critical need for trusted security solutions in government operations and highlights the broader implications for software vendors striving to maintain credibility in a market that increasingly values transparency and reliability in cybersecurity practices.

CyberSecurity Advisors Network

NEWS:

8. Microsoft Power Pages vulnerability exploited in the wild

Original Source: Cybersecurity Dive by Rob Wright

A vulnerability in Microsoft Power Pages has been actively exploited, presenting serious security concerns for users. This flaw allows attackers to execute arbitrary code and potentially take control of affected systems, exposing sensitive data.

The urgency of addressing this issue is paramount, as the exploitation of such vulnerabilities can lead to significant breaches, undermining trust in digital infrastructures. Users are advised to apply patches provided by Microsoft immediately to mitigate the risk and protect their data from unauthorised access.

This situation highlights the ongoing challenges in maintaining secure web environments and the necessity for continuous vigilance and prompt updates in cybersecurity protocols.

CyberSecurity Advisors Network

NEWS:

9. A Data Leak Exposes the Operations of the Chinese Private Firm TopSec, Which Provides Censorship-as-a-Service

Original Source: Security Affairs by Pierluigi Paganini

A significant data leak at TopSec, a Chinese firm known for providing censorship-as-a-service, has exposed extensive details about its operations.

This breach reveals the extent to which the company engages in information control and surveillance for the Chinese government. The exposed data includes sensitive information about the methods and technologies used to monitor and suppress online content.

This incident not only raises concerns about privacy and freedom of expression but also underscores the vulnerabilities in the security practices of companies involved in state-sponsored censorship activities.

The leak prompts a critical examination of the implications for global internet freedom and the ethical responsibilities of technology providers.

CyberSecurity Advisors Network

NEWS:

10. Australia facing higher rate of cyber threats as part of APAC regional surge

Original Source: itWire by Rosalyn Page

Australia is experiencing an elevated rate of cyber threats, part of a broader surge across the Asia-Pacific region. This increase is driven by the escalating sophistication of cyberattacks targeting both public and private sectors.

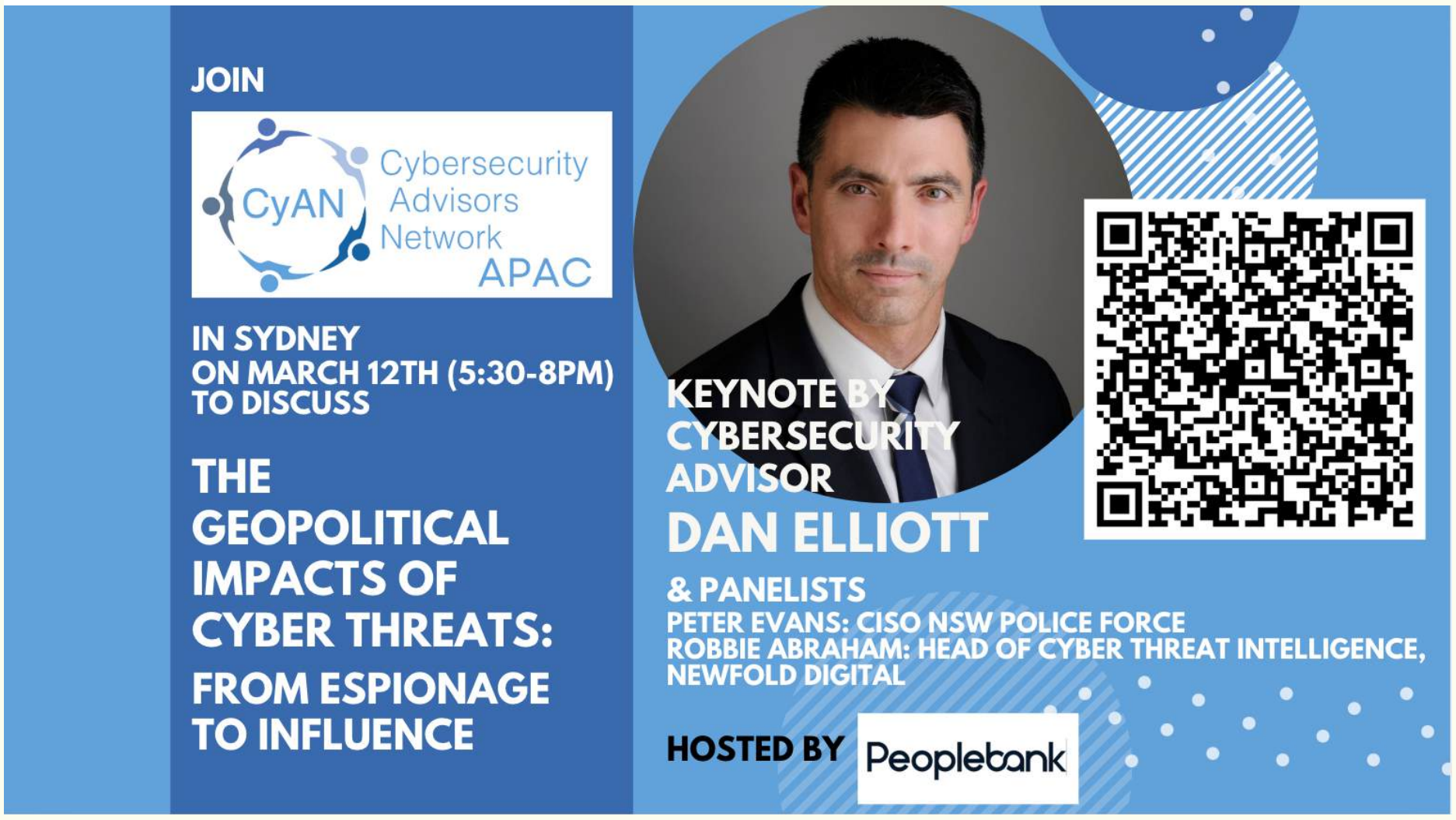
The rise in cyber threats includes phishing, ransomware, and state-sponsored attacks, putting critical infrastructure and data at risk.

This trend necessitates stronger cybersecurity measures, enhanced threat intelligence sharing, and more robust collaboration between government agencies and industry leaders.

The aim is to fortify defences, raise awareness about cyber hygiene practices, and develop more resilient digital ecosystems to counteract the growing cyber threat landscape.

CyberSecurity Advisors Network

SAVE THE DATE!



Mark your calendars—this is one event you won't want to miss!

In a world where cyber threats are reshaping global power dynamics, understanding their geopolitical implications has never been more critical. This event will provide unique insights into how the evolving cyber landscape impacts nations, organisations, and individuals, offering strategies to navigate these challenges with clarity and resilience.

We'll begin with a keynote from acclaimed cybersecurity advisor Dan Elliott, followed by a panel discussion moderated by Dr. Saba Bagheri, Cyber Threat Intelligence Manager at BUPA, featuring

- **Peter Evans, CISO at NSW Police Force**
- **Robbie Abraham, Head of Cyber Threat Intelligence at Newfold Digital**

NEWS:

11. 3.9 Billion Passwords Stolen—Infostealer Malware Blamed

Original Source: Forbes by Davey Winder

In a major cybersecurity alert, Forbes reports that 3.9 billion passwords have been stolen, attributed to a sophisticated infostealer malware.

This breach highlights a severe lapse in digital security protocols globally, prompting an urgent call for heightened cybersecurity measures.

Experts stress the need for robust protective technologies and enhanced user vigilance. They recommend immediate action to upgrade defense systems against such malicious software, which is becoming increasingly capable of evading traditional security checks.

This incident marks a significant moment in cybersecurity, urging a reevaluation of how personal data is protected online.

CyberSecurity Advisors Network

NEWS:

12. Australia fines Telegram for delay in answering questions

Original Source: itNews

Australian regulators have imposed a significant fine on the messaging app Telegram for its delayed response to inquiries regarding its data handling and privacy practices.

This action reflects Australia's stringent approach to enforcing digital communication compliance amid growing concerns over data security. The fine serves as a warning to other tech companies about the importance of quick and transparent responses to regulatory questions.

Experts emphasise that maintaining rigorous data protection standards is crucial for preserving user trust and ensuring compliance with global data privacy laws.

This case highlights the escalating demands on digital platforms to adhere to strict regulatory expectations and the potential repercussions of non-compliance.

CyberSecurity Advisors Network

NEWS:

13. Fake CS2 tournament streams used to steal crypto, Steam accounts

Original Source: BleepingComputer by Bill Toula

Cybercriminals are exploiting the popularity of CS2 tournaments by hosting fake streams that deceive gamers into downloading malware, leading to significant losses of cryptocurrency and Steam accounts.

BleepingComputer reports that these fraudulent streams lure viewers with the promise of live competitive play, only to trick them into installing software that steals sensitive information. This scam highlights the increasing sophistication of cyber threats targeting online gaming communities.

Experts advise gamers to verify the authenticity of streams and download sources, maintain robust security software, and stay informed about common phishing tactics to safeguard their digital and financial assets effectively.

CyberSecurity Advisors Network

NEWS:

14. Former NSA, Cyber Command chief Paul Nakasone says U.S. falling behind its enemies in cyberspace

Original Source: Cyberscoop by Tim Starks

In a candid interview with cyberscoop, former NSA and Cyber Command chief Paul Nakasone expressed concerns that the United States is falling behind its adversaries in cyberspace.

Nakasone emphasised the strategic gaps in America's cyber defences, highlighting that current efforts are insufficient to counteract the sophisticated cyber tactics employed by foreign enemies. Additionally, he highlights a need for a comprehensive national cyber strategy that proactively enhances cybersecurity infrastructure and fosters greater collaboration between government agencies and private sector.

This strategic overhaul, he argues, is essential to maintain national security and to stay ahead in the constantly evolving cyber threat landscape.

CyberSecurity Advisors Network

NEWS:

15. Critical New PayPal Warning: Genuine Emails Used In Ongoing Attack

Original Source: Forbes by Davey Winder

Forbes has issued a critical alert regarding a new phishing scam where attackers are using genuine-looking PayPal emails to execute sophisticated attacks.

This campaign involves cybercriminals crafting emails that mimic official PayPal communications, tricking recipients into divulging sensitive information such as login credentials and financial details. The article stresses the importance of vigilance and educating users on the hallmarks of phishing attempts. It also calls for enhanced email filtering technologies and user education to combat these types of cyber threats effectively.

This incident serves as a stark reminder of the evolving nature of cyberattacks and the need for continuous updates to security measures.

CyberSecurity Advisors Network

NEWS:

16. Beware: PayPal "New Address" feature abused to send phishing emails

Original Source: BleepingComputer by Lawrence Abrams

BleepingComputer reports a new phishing tactic exploiting PayPal's "New Address" feature, where cybercriminals send fraudulent emails urging users to verify their account details. This scam cleverly disguises itself within legitimate-looking PayPal communications, convincing users to input sensitive information, which leads to data breaches and financial loss.

The article highlights the necessity for users to be extremely cautious with email links and to verify any changes through official PayPal channels directly. It also emphasises the importance of ongoing cybersecurity education to recognise and thwart such deceptive techniques, ensuring personal and financial information remains secure.

CyberSecurity Advisors Network

NEWS:

17. NSW finds new permanent cyber chief

Original Source: itNews by Eleanor Dickinson

New South Wales has appointed a new permanent cyber chief to oversee the state's cybersecurity strategy, aiming to strengthen defences against a rising tide of cyber threats.

This appointment underscores the growing recognition of the critical importance of cybersecurity at the state level.

The new cyber chief's role will focus on enhancing collaboration between government agencies, bolstering cyber incident response capabilities, and developing comprehensive policies to protect public and private sector data.

This strategic move is part of a broader effort to fortify digital infrastructure and ensure robust protection for citizens' data in the face of increasingly sophisticated cyberattacks.

CyberSecurity Advisors Network

NEWS:

18. Hackers steal $1.5bn from crypto exchange in ‘biggest digital heist ever’

Original Source: The Guardian by Joanna Partridge

The Guardian reports a monumental theft where hackers stole $1.5 billion from a cryptocurrency exchange, marking it as the biggest digital heist in history.

This staggering breach involved sophisticated cyber tactics that overcame existing security measures, prompting a global reevaluation of cryptocurrency security protocols. The incident has sent shockwaves through the financial technology industry, highlighting vulnerabilities that could potentially expose other platforms.

Experts are now calling for heightened security measures, including advanced encryption and multi-factor authentication, to protect against similar attacks and to reassure the increasingly anxious investor community about the safety of their digital assets.

CyberSecurity Advisors Network

NEWS:

19. DOGE Sparks Surveillance Fear Across the US Government

Original Source: Wired by Paresh Dave, Dell Cameron & Alexa O’Brien

Wired reports escalating concerns within the US government regarding the cryptocurrency DOGE and its potential use in surveillance and data collection. These fears stem from DOGE's rapid integration into mainstream financial systems and its accessibility to top cybersecurity agencies.

Government officials are debating the implications of such technologies, which could potentially be exploited for mass surveillance or violate privacy rights.

This issue highlights the ongoing tension between technological innovation and civil liberties, prompting a call for strict regulatory frameworks to govern the use of cryptocurrencies in government operations while safeguarding individual privacy.

CyberSecurity Advisors Network

NEWS:

20. Telegram fined nearly $1m by Australian watchdog for delay in reporting about terrorism and child abuse material

Original Source: The Guardian by Josh Taylor

Australian regulators have imposed a fine of nearly $1 million on Telegram for its delayed action in reporting incidents involving terrorism and child abuse material.

This penalty emphasises the critical role social media platforms play in preventing the spread of harmful content. It also spotlights the stringent expectations from authorities worldwide that platforms enforce proactive monitoring and swift reporting practices.

The case serves as a caution to other companies about the severe consequences of failing to adhere to legal and ethical standards in content management.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

Register Now!

Breaking the Cycle: Combating Online IBSA for a Safer Digital Experience

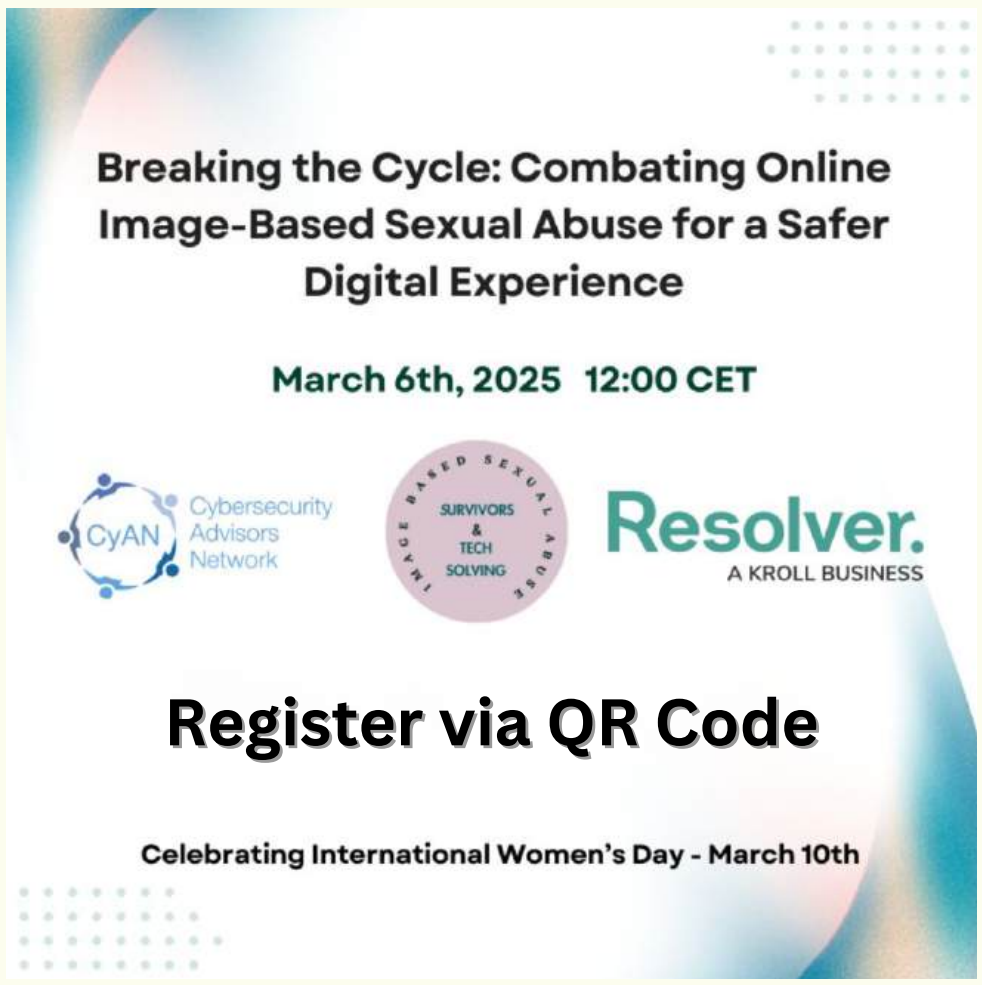


Image-Based Sexual Abuse (IBSA) is a growing threat—one that deeply impacts individuals, communities, and the very fabric of online trust. It's time to take action.

Join Cybersecurity Advisors Network (CyAN), Resolver Trust & Safety, and STISA (Survivors & Tech Solving Image-based Sexual Abuse) for a powerful webinar that brings together leading experts and changemakers to tackle this urgent issue head-on.

This webinar will feature speakers:
Caroline Humer, Henry 'H' Adams, Robbert Hoving, Dr Silvia Semenzin and CyAN's Kim Chandler McDonald

NEWS:

21. Apple removes advanced data protection tool in face of UK government request

Original Source: The Guardian by Rachel Hall

In response to a UK government request, Apple has removed an advanced data protection tool from its products in the UK, a move that has sparked widespread concerns over privacy.

This action highlights the ongoing struggle between government surveillance needs and individual privacy rights.

Critics and privacy advocates are alarmed, suggesting that this could undermine user trust and set a troubling precedent for tech companies, potentially eroding privacy protections globally.

The debate continues about the balance that needs to be struck between national security and protecting citizens' private data.

[Ed note: For further analysis of this subject see item #23, '*Apple's Bold Move in the UK: No Backdoor, No Extra Encryption*]'

CyberSecurity Advisors Network

NEWS:

22. DOGE Now Has Access to the Top US Cybersecurity Agency

Original Source: Wired by Kim Zetter

Wired reveals that the cryptocurrency DOGE has gained unprecedented access to a top U.S. cybersecurity agency, stirring debates over the implications for national security and privacy.

This development comes as government entities increasingly explore the potential of blockchain technologies for enhancing security operations. However, the integration of DOGE raises concerns about the security and transparency of governmental use of cryptocurrency technologies.

Critics argue this could lead to potential vulnerabilities, calling for rigorous oversight and clear guidelines to ensure that such technologies do not compromise the integrity of national security measures.

CyberSecurity Advisors Network

ANALYSIS:

23. Apple’s Bold Move in the UK: No Backdoor, No Extra Encryption

Original Source: PrivID (Substack)

In a decisive stance, Apple has opted not to include additional encryption or backdoor access in its UK products, as reported by PrivID on Substack.

This decision highlights Apple's commitment to user privacy amidst pressure from the UK government to allow backdoor access for law enforcement purposes.

The article elaborates on the broader implications of this move for privacy advocacy and cybersecurity, arguing that resisting government pressure helps maintain trust and security for users globally. It discusses the potential consequences for Apple in terms of legal challenges and market dynamics, emphasising the delicate balance between national security demands and the preservation of individual privacy rights.

CyberSecurity Advisors Network

ANALYSIS:

24. Cybersecurity Needs to Stay Nonpartisan in the Age of DOGE

Original Source: Lohrmann on Cybersecurity by Dan Lohrmann

In his commentary for "Lohrmann on Cybersecurity," Dan Lohrmann stresses the importance of nonpartisanship in cybersecurity, particularly as the influence of cryptocurrencies like DOGE grows within national security frameworks.

According to Lohrmann, the entanglement of digital currencies with security issues could lead to political exploitation. He advocates for a bipartisan approach to cybersecurity, urging that policies and actions should transcend political divisions to effectively protect national interests.

Lohrmann argues that cybersecurity resilience depends on collaborative efforts and adherence to shared principles, rather than being influenced by fluctuating political agendas.

CyberSecurity Advisors Network

ANALYSIS:

25. Cybersecurity in 2025: A battle of interwoven interests

Original Source: The Peninsula by Dr. Khaled Walid Mahmoud

Dr. Khaled Walid Mahmoud's article in The Peninsula addresses critical challenges in the cybersecurity landscape of 2025, particularly emphasising the growing resilience disparity between large and small institutions. He highlights how smaller entities often lack the resources to implement comprehensive cyber defenses, making them particularly vulnerable to attacks.

Amidst this scenario, Dr. Mahmoud poses an essential question regarding the position of Arab nations within the global cybersecurity equation. He discusses their unique vulnerabilities and the need for regional cooperation to enhance security frameworks and reduce disparities.

This dialogue is crucial as it underscores the importance of tailored cybersecurity strategies that account for varied economic and technological capabilities across different regions.

CyberSecurity Advisors Network

ANALYSIS:

26. Cyber Insurance is Useless Without Encryption

Original Source: PrivID (Substack)

This PrivID article highlights a crucial aspect of cyber risk management: the ineffectiveness of cyber insurance without robust encryption practices.

As cyber threats evolve, merely relying on insurance policies without securing data at its core leaves organisations vulnerable.

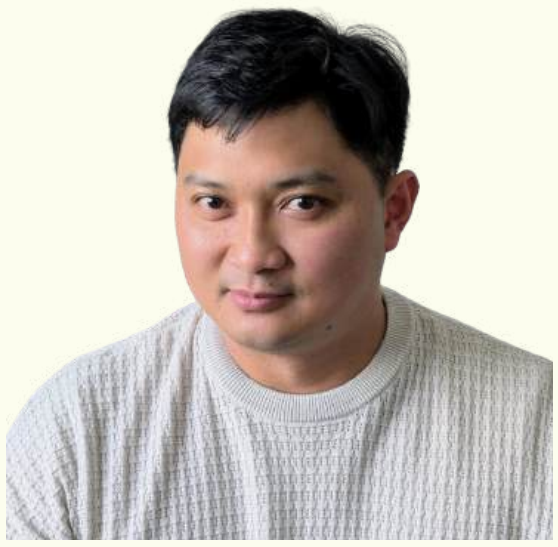
The piece emphasises that encryption is essential not just for safeguarding data but also for meeting the stringent requirements that insurance policies increasingly demand. It calls on organizations, particularly SMEs, to integrate strong encryption methods as a standard practice to enhance their overall cybersecurity measures and ensure that they are genuinely protected against potential breaches.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

27. The 3 Levels of Threat Intelligence: How They Help You Stay Secure

By CyAN Member & General Secretary, Fel Gayanilo



In this insightful piece, CyAN General Secretary Fel Gayanilo breaks down threat intelligence into three distinct levels—strategic, tactical, and operational. Fel explains how each level plays a crucial role in enhancing an organisation's cybersecurity posture.

Strategic threat intelligence helps in understanding the broad risk landscape, tactical intelligence focuses on immediate threats, and operational intelligence deals with day-to-day security events.

This layered approach, Fel argues, enables organizations to better anticipate potential threats and tailor their defenses accordingly, thereby staying one step ahead of cyber adversaries.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

28. Quantum Computing and the Urgent Need for Universal End-to-End Encryption

By CyAN Global VP Kim Chandler McDonald

CyAN VP Kim Chandler McDonald discusses the transformative impact of quantum computing on cybersecurity, particularly stressing the urgent need for universal end-to-end encryption.

Kim highlights how quantum computing poses significant risks to current encryption methods and could potentially break many of the cryptographic systems currently in use.

The article calls for proactive measures to develop quantum-resistant encryption technologies to protect data against future threats.

Kim's insights underline the importance of preparing for quantum advancements to ensure privacy and security in the digital age.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

29. Smart Security Everywhere: Empowering CXOs with Always-On Protection

By CyAN Member & IMNIS Mentor Shantanu Bhattacharya

CyAN member Shantanu Bhattacharya addresses the need for comprehensive security solutions in his article on ‘Smart Security Everywhere’.

Strongly advocating for an 'Always-On' protection model that empowers CXOs to manage and mitigate risks continuously, Shantanu outlines how integrating smart security technologies across all organisational levels can provide real-time threat detection and response, thus safeguarding critical assets.

His recommendations emphasise the role of leadership in fostering a culture of security that aligns with business objectives and adapts to the evolving cyber threat landscape.

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!

With that in mind, please join us in congratulating our valued member Krishna Pasumarthi on achieving the ISO 42001 Lead Auditor certification!

At CyAN, we recognize the dedication and expertise required to attain such a significant credential, especially in the evolving landscape of AI governance and cybersecurity. Krishna's commitment to continuous learning and resilience, taking the exam at 3 AM. This exemplifies the qualities of a true cybersecurity leader!

CyberSecurity Advisors Network

UPCOMING EVENTS:

- **Breaking the Cycle: Combating Online IBSA for a Safer Digital Experience webinar, March 6th (EST 6AM, CET 12PM, AEST 10PM)**
- **CyAN APAC: The Geopolitical Impacts of Cyber Threats: From Espionage to Influence keynote by Dan Elliot, March 12, Peoplebank, Sydney (save the date, more info on page 10 of this newsletter!)**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April**
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April**
- **GISEC: Dubai Word Trade Center, Dubai, UAE: 6- 8 May**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK**
- **World AI Technology Expo UAE, Dubai, UAE: 14-15 May 2025 https://worldaiexpo.i**
- **MaTeCC, Rabat, Morocco: 7-9 June, 2025 hosted by CyAN partner organisation École High-Tech.**

CyAN Mentorship Program 2025:

At CyAN, we believe mentorship is a powerful tool to nurture future leaders and strengthen our global community.

Our structured three-month mentorship program offers professional guidance, international networking opportunities, and real-world insights tailored to support graduate students and early-career professionals.

By connecting with experienced CyAN members, mentees gain invaluable skills and perspectives to advance their careers.

If you're ready to grow, learn, and thrive alongside experts in cybersecurity and trust & safety, we encourage you to join this transformative opportunity.

FULLY BOOKED!

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