CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #111

NEWS:

1. Russia arrests one of its own – a cybercrime suspect on FBI's most wanted list

Original Source: The Register by Connor Jones

Russia arrests one of its own – a cybercrime suspect on FBI's most wanted list |Russia has detained a high-profile cybercriminal who was on the FBI's most-wanted list.

This rare collaboration between the U.S. and Russia marks a significant development in combating transnational cybercrime. While details of the arrest remain sparse, experts speculate it could signal a strategic shift in Russia's approach to international cybercrime.

The move underscores the growing pressure on nations to address cyber threats that transcend borders. However, long-term cooperation remains uncertain amid geopolitical tensions.

CyAN Cybersecurity Advisors Network

NEWS:

2. Meta plans to build a $10B subsea cable spanning the world, sources say

Original Source: TechCrunch by Ingrid Lunden

Meta is reportedly planning a $10 billion subsea cable project designed to improve global connectivity and support its metaverse ambitions.

The massive undertaking highlights the tech giant's commitment to data infrastructure and its role in driving internet access worldwide. Critics, however, raise concerns over data sovereignty and the environmental impact of such large-scale projects.

If completed, the cable will mark a major milestone in enhancing internet capacity, with significant implications for global digital transformation.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

3. National security watchdog mulls new limits on hacking powers

Original Source: InnovationAus by Justin Hendry

Australia's Inspector-General of Intelligence and Security is considering stricter controls on government hacking powers following public backlash.

The review comes amid concerns over privacy and the potential misuse of hacking tools by intelligence agencies. Advocacy groups argue for greater oversight and transparency, emphasising the need to balance national security with civil liberties.

The outcome of this review could set a precedent for how democratic nations address the ethical implications of state-sponsored hacking.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

4. Warning: Patch Advantech Industrial Wireless Access Points

Original Source: SMG Data Breach Today by Prajeet Nair

A critical vulnerability in Advantech Industrial Wireless Access Points has prompted an urgent patch advisory to prevent exploitation.

The flaw could allow attackers to infiltrate industrial networks, posing risks to critical infrastructure. Security researchers stress the importance of immediate action to protect against potential breaches.

This incident highlights the ongoing challenges of securing industrial IoT devices, particularly as cyber threats continue to evolve in complexity and impact.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

5. Telcos required to block or flag scam texts under Labor crackdown

Original Source: The Guardian by Paul Karp

Australia’s Labor government has introduced new measures requiring telcos to block or flag scam texts in real-time.

The initiative is part of a broader crackdown on fraud targeting mobile users. Experts applaud the move but warn that robust implementation will be key to its success.

Telcos face challenges in balancing security measures with user privacy, while scammers continue to innovate. The policy reflects growing efforts to combat cybercrime at the infrastructure level, setting a potential example for other nations.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

6. The workplace has become a surveillance state

Original Source: The Register by Thomas Claburn

Workplace surveillance is on the rise, with employers leveraging advanced tools to monitor employees' productivity, communications, and even keystrokes.

Critics warn that this trend erodes trust and privacy, creating a "surveillance state" in corporate settings. While organisations argue these measures boost efficiency and security, experts highlight the psychological toll on workers and potential legal ramifications.

Striking a balance between monitoring and respecting employee rights is becoming a key challenge in the modern workplace.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

7. “Rockstar 2FA” Phishing-as-a-Service Steals Microsoft 365 Credentials Via AiTM Attacks

Original Source: Cyber Security News by Balaji N

A new phishing-as-a-service campaign, dubbed "Rockstar 2FA," is using adversary-in-the-middle (AiTM) attacks to bypass multi-factor authentication and steal Microsoft 365 credentials.

The service is being marketed to cybercriminals, lowering the technical barrier to sophisticated attacks. Researchers warn organisations to implement robust email security measures and adopt phishing-resistant MFA methods.

This case underscores the evolving nature of phishing threats and the urgent need for organisations to stay ahead of attackers.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

8. AWS launches an incident response service to combat cybersecurity threats

Original Source:

AWS has unveiled a new incident response service aimed at helping customers navigate cybersecurity crises more effectively. The service offers automated threat detection, real-time insights, and expert support to minimise downtime and damage.

Analysts see this as a strategic move to strengthen AWS's position in the cybersecurity market, though it also highlights the increasing complexity of cloud security.

Organisations are encouraged to integrate such services into their broader security strategies to enhance resilience against evolving threats.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

9. INTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million

Original Source: Interpol

Interpol’s latest crackdown on financial cybercrime has resulted in 5,500 arrests and the seizure of $400 million in assets.

The operation targeted phishing scams, money laundering, and other forms of digital fraud across 30 countries. Authorities credit international cooperation for the operation's success, underscoring the global nature of cybercrime.

Experts highlight the need for continued cross-border collaboration to disrupt criminal networks and strengthen global financial security.

CyberSecurity Advisors Network

10. Alder Hey children's hospital explores 'data breach' after ransomware claims

Original Source: The Guardian by Dan Milmo & Andrew Gregory

Alder Hey Children's Hospital is investigating claims of a ransomware attack that allegedly compromised patient data.

While the hospital has yet to confirm the breach, experts warn that healthcare institutions remain prime targets for cybercriminals due to their sensitive data and critical operations.

The incident underscores the importance of robust cybersecurity measures in healthcare, including timely patching, incident response planning, and employee training.

Investigations are ongoing to assess the extent of the damage.

CyberSecurity Advisors Network

NEWS:

11. New Windows Cyber Attack Warning As 0-Click Russian Backdoor Confirmed

Original Source: Forbes by Davey Winder

Security researchers have confirmed the existence of a 0-click backdoor targeting Windows systems, attributed to a Russian-linked cybercriminal group.

The backdoor allows attackers to gain access without user interaction, posing significant risks to organisations globally. Microsoft has released patches to address the vulnerability, urging users to update systems immediately.

This attack highlights the evolving sophistication of cyber threats and the need for proactive monitoring and patch management to safeguard critical infrastructure.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

12. RansomHub claims to net data hat-trick against Bologna FC

Original Source: The Register by Connor Jones

RansomHub, a ransomware gang, claims to have stolen sensitive data from Bologna FC in a high-profile cyberattack targeting the football club.

The breach reportedly includes financial and operational data, putting the organisation at risk of reputational and legal fallout.

Experts warn that sports organisations, often seen as soft targets, need to prioritise cybersecurity. The incident underscores the growing trend of ransomware groups targeting non-traditional sectors to maximise impact and leverage.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

13. Zabbix urges upgrades after critical SQL injection bug disclosure

Original Source: The Register by Connor Jones

Zabbix, a popular open-source monitoring tool, has disclosed a critical SQL injection vulnerability that could allow attackers to gain unauthorised access to sensitive systems.

Users are urged to upgrade to the latest version immediately to mitigate potential exploitation. This incident highlights the persistent risks associated with third-party software vulnerabilities and the need for timely updates.

Organisations relying on Zabbix for monitoring must act swiftly to protect against potential breaches.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

14. Uganda confirms hack of central bank accounts, official downplays extent of loss

Original Source: Reuters by Elias Biryabarema

Uganda has confirmed a cyberattack on its central bank accounts, with officials stating the financial impact is limited. However, the incident raises concerns about the security of critical financial systems in developing nations.

Experts highlight the importance of robust cybersecurity measures and international cooperation to protect against increasingly sophisticated threats.

This case underscores the need for financial institutions to prioritise resilience and incident response planning in the face of growing cyber risks.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

15. Trump will take a largely deregulatory approach to tech, while aiming to aggressively pursue foreign cyber threat actors

Original Source: Governing by Jule Pattison-Gordon

Former President Trump's anticipated return to office could bring a deregulatory approach to the tech industry, prioritising reduced compliance burdens for businesses. However, his administration is also expected to intensify efforts against foreign cyber threats, particularly those from adversarial nations.

Analysts warn that deregulation could weaken safeguards, while aggressive policies against cyber actors may escalate geopolitical tensions. The tech sector faces a complex mix of opportunities and challenges under this potential policy direction.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

ANALYSIS:

16. Researchers Say Here’s How To Prepare Now For Post Quantum Cybersecurity

Original Source: Quantum Insider by Matt Swayne

Post-quantum cybersecurity is becoming a critical focus as quantum computing advances threaten current encryption methods.

Researchers recommend transitioning to quantum-resistant algorithms and preparing for hybrid encryption solutions to ensure long-term data security. Organisations are urged to assess their cryptographic dependencies and plan proactive migrations.

This transition highlights the growing importance of staying ahead of technological disruptions to safeguard sensitive information in a rapidly evolving digital landscape.

CyberSecurity Advisors Network

ANALYSIS:

17. Telco security is a dumpster fire and everyone's getting burned

Original Source: The Register by Rupert Goodwins

Telco security vulnerabilities are becoming increasingly apparent, exposing both consumers and organisations to risks ranging from data breaches to service outages. T

his opinion piece explores the systemic flaws in the telco sector, including outdated infrastructure and insufficient regulations. Experts call for comprehensive reforms, urging telcos to adopt zero-trust principles and robust incident response protocols.

Addressing these issues is essential to restore trust and resilience in a critical industry supporting global connectivity.

CyAN
Cybersecurity
Advisors
Network

CyAN Member's Features:

18. The Importance of Tech Allies in the 16 Days of Activism

Original Source: Kim Chandler McDonald

In this piece, CyAN member Kim Chandler McDonald highlights the pivotal role of technology in combating gender-based violence during the 16 Days of Activism.

From secure communication tools to AI-driven abuse detection, technology offers solutions to empower victims and hold perpetrators accountable. However, the article stresses the importance of ethical design and robust privacy measures to prevent misuse.

Building a safer digital environment requires collaboration among technologists, advocates, and policymakers.

Cybersecurity Advisors Network

CyAN Member's Features:

19. Empowering Developers Through Security Training: The Role of Secure Coding and Threat Modeling (and a hat-tip to Microsoft!)

Original Source: Nick Kelly

In this article, CyAN member Nick Kelly advocates for empowering developers with security training, focusing on secure coding practices and threat modelling.

Highlighting Microsoft's initiatives as an example, the piece emphasises how equipping developers with the right tools and knowledge can significantly reduce vulnerabilities.

Bridging the gap between development and security is essential to building resilient systems, fostering a culture of collaboration and proactive defence against cyber threats.

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!

CyAN Cybersecurity Advisors Network

UPCOMING CyAN EVENTS

- **MaTeCC: Rabat, Morocco: 7-9 June, 2025**
- **GITEX AFRICA, Marrakesh, Morocco: 14 - 16 April, 2025**

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!

#SharingIsCaring