CyAN
Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #104

Cybersecurity Advisors Network

NEWS:

1. 24% of CISOs actively looking to leave their jobs

Original Source: CSO Online by Evan Schuman

A recent survey reveals that 24% of Chief Information Security Officers (CISOs) are actively seeking new job opportunities, with many others contemplating leaving within three years due to extreme stress, insufficient executive support, and intense workloads.

This trend poses a significant risk to organisations, as CISOs play a crucial role in managing cybersecurity threats and protecting sensitive data. Many CISOs report a disconnect with board-level leaders who may undervalue cybersecurity's strategic importance. The findings highlight an urgent need for organisational change to ensure CISO support and long-term retention through balanced workloads and mental health resources.

Cybersecurity Advisors Network

CyAN

NEWS:

2. Cyberattacks hit 1 in 3 SMBs last year

Original Source: Cybersecurity Dive by Matt Kapko

One in three small and medium-sized businesses (SMBs) experienced a cyberattack in the past year, showcasing the vulnerability of this sector. With limited resources and often lacking dedicated cybersecurity staff, SMBs remain frequent targets for ransomware, phishing, and other attacks.

The report reveals that attacks led to costly downtime and financial loss, highlighting the pressing need for SMBs to prioritise cybersecurity. As attacks on SMBs rise, a proactive approach to cybersecurity, including employee training and affordable security tools, could be essential to protect both their operations and reputations in an increasingly digitised economy.

Cybersecurity Advisors Network

CyAN

NEWS:

3. German Law Could Protect Researchers Reporting Vulns

Original Source: Dark Reading

Germany is drafting a law to protect security researchers who responsibly report software vulnerabilities, aiming to establish legal safeguards against potential prosecution. This legislation encourages ethical hacking by allowing researchers to identify and disclose vulnerabilities without facing legal risks.

By supporting responsible vulnerability disclosure, the German government is promoting a collaborative approach to cybersecurity, enhancing both public and private digital safety. This progressive stance could serve as a model for other countries, encouraging a safer and more transparent cybersecurity environment while safeguarding researchers who work to uncover and mitigate security threats.

CyAN Cybersecurity Advisors Network

NEWS:

4. Canada Is Doing Its Own Extremely Weird TikTok Ban

Original Source: CSO Online by Evan Schuman

Canada has introduced an unusual approach to restricting TikTok, banning government employees from using the app on official devices, while allowing citizens to continue using it. The decision stems from concerns over data privacy and potential foreign influence due to TikTok's ties to China.

Despite these concerns, Canada's partial ban has sparked debate about its effectiveness, as the government has not extended the ban to the general public or other widely-used apps with similar risks. This selective approach raises questions about the consistency and impact of such restrictions, with some viewing it as an insufficient step toward addressing broader data privacy issues.

CyAN Cybersecurity Advisors Network

NEWS:

5. Suspect behind Snowflake data-theft attacks arrested in Canada

Original Source: BleepingComputer by Sergiu Gatlan

In more news from Canada, Canadian authorities recently arrested a suspect allegedly responsible for multiple cyberattacks targeting data on the Snowflake platform. The individual reportedly accessed and exfiltrated sensitive customer data, sparking industry-wide concerns about cloud security and data protection.

Snowflake responded by tightening security measures and promptly notifying impacted clients. This arrest underscores the importance of robust data security protocols within cloud services, as breaches have severe implications for customer trust and business continuity, emphasising the need for heightened vigilance across cloud-based platforms.

6. Interpol disrupts cybercrime activity on 22,000 IP addresses

Original Source: Security Affairs by Pierluigi Paganini

In a major crackdown, Interpol’s Operation Synergia II dismantled over 22,000 IP addresses involved in cybercriminal activities, including fraud, ransomware, and various malicious campaigns.

The operation targeted an international network of cybercriminals, reflecting the increasingly global approach required to combat online threats. By neutralising these IPs, Interpol aims to disrupt illicit operations that threaten digital security on a broad scale, highlighting the critical role of international collaboration in defending against cybercrime.

7. China state-linked group accused of hacking SingTel

Original Source: itNews

A Chinese state-linked hacking group is accused of breaching SingTel, Singapore’s leading telecom provider, raising concerns about cybersecurity risks within essential infrastructure.

The attackers reportedly accessed sensitive data, which has amplified fears about state-sponsored attacks targeting critical telecom networks in Asia. This breach underscores the urgent need for advanced cybersecurity defences within the telecom sector, especially as state-affiliated actors increasingly turn their focus on pivotal infrastructure providers.

Cybersecurity Advisors Network

CyAN

NEWS:

8. Google fixes two Android zero-days used in targeted attacks

Original Source: Bleeping Computer by Bill Toulas

Google has released patches for two critical zero-day vulnerabilities in its Android operating system that were actively exploited in targeted attacks. These zero-day flaws, affecting Android's core components, allowed attackers to gain privileged access to devices, putting users at risk of data breaches and unauthorised access.

Google's rapid response underscores the importance of timely updates to protect against increasingly sophisticated threats. Users are urged to install the latest security updates promptly to mitigate the risk from these vulnerabilities, which highlight ongoing challenges in securing mobile operating systems.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

9. Police Doxing of Criminals Raising Ransomware-Attack Stakes

Original Source: ISMG Data Breach Today by Mathew Schwartz

The controversial strategy of law enforcement “doxing” cybercriminals—publicly revealing their personal information to deter further attacks—has prompted an escalation in ransomware retaliation tactics. While proponents argue that exposing these criminals can help curb cyber threats, critics warn that doxing may provoke more aggressive and unpredictable behavior from ransomware gangs.

In response, some cybercriminals have intensified their attacks, targeting law enforcement and escalating threats against public and private sector entities. This evolving situation raises important ethical questions, as well as practical concerns about whether doxing truly helps to reduce cybercrime or if it ultimately leads to increased risks for organisations and law enforcement alike.

CyberSecurity Advisors Network

10. Schneider Electric confirms dev platform breach after hacker steals data

Original Source: BleepingComputer by Lawrence Abrams

Schneider Electric recently reported a security breach on its development platform, with hackers managing to access and steal sensitive data. This incident spotlights vulnerabilities in development environments, particularly within industrial and infrastructure-critical sectors, where breaches can have severe operational consequences.

In response to the attack, Schneider Electric has strengthened its security measures, including tightening access controls and enhancing monitoring protocols to detect future threats. The breach underscores the importance of securing development platforms, as these environments are often targeted for their role in essential operational processes, making them a prime focus for attackers seeking to disrupt critical infrastructure.

Cybersecurity Advisors Network

NEWS

11. Schneider Electric ransomware crew demands $125k paid in baguettes

Original Source: The Register by Jessica Lyons

Other Schneider news... the ransomware group targeting Schneider Electric has demanded a ransom of $125,000 in the form of baguettes.

While this strange demand could be viewed as an intimidation tactic or an attempt to gain attention, it reveals the lengths to which ransomware groups will go to manipulate or disrupt their targets.

The bizarre request highlights the unpredictable nature of modern ransomware attacks, reminding organisations of the importance of preparedness for unconventional threats.

CyAN Cybersecurity Advisors Network

NEWS:

12. Google Researchers Claim First Vulnerability Found Using AI

Original Source: Infosecurity Magazine by Kevin Poireault

In a significant breakthrough, Google researchers have leveraged artificial intelligence to discover a previously unknown vulnerability, marking a new chapter in AI-driven cybersecurity.

This accomplishment demonstrates AI's potential in proactively identifying security flaws that may be overlooked by traditional detection methods. By automating vulnerability identification, AI could improve both the speed and accuracy of threat detection, helping organisations to stay ahead of emerging risks.

This advance signals a shift in cybersecurity, where AI may increasingly play a central role in safeguarding systems and data, enhancing both preventative measures and real-time security responses.

CyAN Cybersecurity Advisors Network

Trust in Focus

Unpacking Key Topics In The Digital Age

In this month's Trust in Focus segment, we turn our attention to the critical role of cybersecurity in protecting individuals from technology-facilitated abuse.

As digital tools increasingly intersect with personal and public safety, it's essential to consider how technology can both empower and, at times, enable harmful behaviours such as stalking, online bullying, and surveillance. These articles explore the impact of cyber-enabled abuse, the strategies for safeguarding privacy, and the essential responsibilities of platforms and policies to uphold user safety and trust in a digital world.

CyAN Cybersecurity Advisors Network

Trust in Focus:

13. Risk, Compliance, and the Fight Against Technology-Facilitated Domestic Violence: A Critical Intersection

Original Source: Risky Women by Kim Chandler McDonald

This article explores the intersection of cybersecurity, risk management, and the fight against technology-facilitated domestic violence (TFDV). It highlights how organisations, through compliance and governance, can help combat digital abuse by implementing policies that protect victims from surveillance and control.

As abusers increasingly weaponise technology, there is a growing need for collaboration among legal, cybersecurity, and social sectors to create protective frameworks. This piece underscores the ethical responsibility of the cybersecurity industry in safeguarding individuals and highlights TFDV as a pressing human rights issue that requires immediate and coordinated action.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

Trust in Focus:

14. Domestic violence: Is your smartphone being tracked? Here's how to tell

Original Source: The Guardian by Ariel Bogle

Ariel Bogle's practical guide in The Guardian provides crucial insights for individuals who suspect they may be victims of smartphone tracking—a method frequently employed in cases of technology-facilitated domestic abuse.

The article details the warning signs of tracking apps and offers step-by-step guidance on adjusting privacy settings to guard against unauthorised surveillance. This resource is especially important as it empowers those affected by TFDV to reclaim control of their digital lives, encouraging awareness and practical action.

By equipping readers with this knowledge, the guide fosters self-protection and reinforces the need for enhanced public awareness on digital privacy risks in abusive situations

CyberSecurity Advisors Network

Trust in Focus:

15. X updates block feature, letting blocked users see your public posts

Original Source: Tech Crunch by Ivan Mehta

In a controversial move, X (formerly Twitter) has updated its block feature to allow blocked users to view public posts, sparking widespread concerns about user safety. Critics argue this change undermines a vital safety mechanism, particularly for individuals facing harassment or abuse, who rely on blocking to shield themselves.

The update raises important questions about the platform's responsibility to balance open content access with the need for user protection. For many users, this change signifies a potential erosion of personal control and privacy, prompting a re-evaluation of how social media platforms approach safety, trust, and digital rights in their policies.

Cybersecurity Advisors Network

CyAN

Trust in Focus:

16. Australia to ban under-16s from social media – but can't say how TikTok, Instagram and others will enforce it

Original Source: Tech Crunch by Ivan Mehta

The Australian government has announced plans to introduce legislation setting a minimum age limit of 16 for social media use. This move aims to protect young people from online harms, aligning with broader efforts to enhance digital safety for minors.

However, the government has not clarified how social media companies will verify users' ages, raising questions about the feasibility of enforcement. While age limits have been touted as a necessary step to curb exposure to inappropriate content and online risks, critics argue that without robust enforcement mechanisms, the legislation may lack effectiveness in achieving its intended protections.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

Trust in Focus:

17. Combatting Technology-Facilitated Abuse and Violence: A Call to Action

Original Source: Cybersecurity Advisors Network (CyAN) by Kim Chandler McDonald and Vaishnavi J

This CyAN call-to-action, originally published on May 5th, 2024, highlights the increasing prevalence of technology-facilitated abuse and violence (TFAV), urging cybersecurity professionals, policymakers, and organisations to take immediate, coordinated action. TFAV encompasses a range of abuses—including online harassment, stalking, and coercive control—exacerbated by digital tools that enable perpetrators to monitor, manipulate, and intimidate victims.

The article underscores the need for robust policy frameworks, specialised cybersecurity tools, and public education to protect vulnerable individuals from digital abuse. It calls on the tech industry to lead efforts in developing safeguards and to recognise that protecting individuals from TFAV is integral to maintaining a safe and trusted digital ecosystem

Cybersecurity Advisors Network

UPCOMING CyAN EVENTS

Dubai: November 20-21
Third Party & Supply Chain Cyber Security Summit
Sydney: November 27
Women (and their allies!) in Cyber

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

#ReallyInterestingCyberStuff!