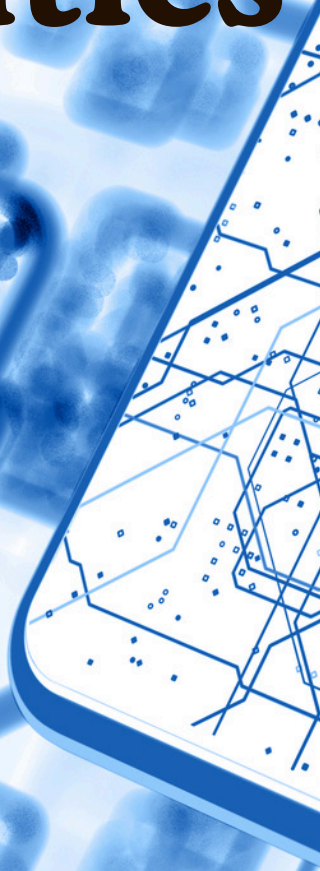
CyAN Cybersecurity Advisors Network

Cyber (In)Securities Issue #175



Enterprise IT World MEA Hosts 4th Achievers X Awards in Dubai, Honouring 100 IT and Security Leaders

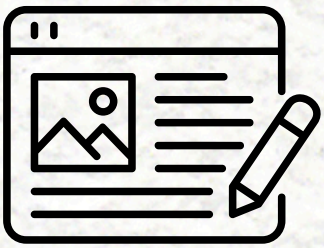
Enterprise IT World MEA | October 15 2025

The 4th edition of the Achievers X Awards took place at the Shangri-La Dubai, celebrating the region's top 100 IT and cybersecurity leaders. Supported by Infoblox, Nohac.ai, Seceon, and Cache Digitech, the event recognised excellence and innovation across industries such as BFSI, healthcare, education, retail, and manufacturing.

Highlights included an inspiring keynote by Akash Sureka, Founder of TheNoah.ai, on low-code AI frameworks, and a fireside chat between **Bharat Raigangar** (CyAN Board Advisor and vCISO) and Sandip Wadje (BNP Paribas), exploring AI-driven security models and emerging operational risks.

Hosted by Accent Info Media's Sanjay and Sanjib Mohapatra, the ceremony honoured exceptional CIOs, CISOs, CDOs, and AI leaders who continue to shape the MEA technology landscape. The evening concluded with a gala dinner and networking session, reinforcing the event's mission to celebrate leadership and collaboration in enterprise tech.

CyAN Cybersecurity Advisors Network



BLOG, ARTICLES & PODCAST

Germany's Privacy Win: Why It Matters for International Data Week

Digital governance isn't just about frameworks and policies, it's about people, power, and the principles we're willing to defend when technology overreaches.

And this week, as delegates gather for International Data Week 2025 in Brisbane, they do so against the backdrop of a significant win for digital privacy: Germany's decision to block the European Union's controversial "Chat Control" proposal.

The proposal, formally known as the Child Sexual Abuse Regulation, would have required messaging platforms to scan users' content for illegal material before it's encrypted. On paper, it was about protecting children. In practice, it risked undermining encryption entirely.

Germany's refusal to back the proposal stopped it in its tracks. It's a quiet but powerful victory for data privacy, encryption, and the citizens who made their voices heard.

A Turning Point for Digital Privacy

Over 500 cryptographers and researchers across 34 countries signed open letters warning that "Chat Control" was technically infeasible and dangerously intrusive. Civil society campaigns gathered momentum. And in the end, citizen protest tipped the balance: Berlin could no longer ignore the message that privacy isn't a privilege; it's a right.

Patrick Breyer, the digital rights advocate who helped lead the charge, called the decision "a major victory for digital privacy." He's right. It's not just a win for Germany or the EU, it's a reaffirmation that digital safety can't come at the cost of universal surveillance.

What makes this moment especially important is its timing. Just as the global data community meets to discuss how to manage, share, and protect data responsibly, Germany's stance reminds us that privacy and governance are inseparable. There's no trustworthy data ecosystem without trust itself.

Trust, Encryption, and the Myth of Safety by Surveillance

Encryption isn't an obstacle to safety; it's the foundation of it. Weakening it in the name of protection doesn't make people safer – it just opens the door to new risks, abuses, and backdoors that bad actors will inevitably exploit.

Germany's rejection of the proposal recognises a reality many policymakers still struggle to grasp: safety and privacy are not opposing forces. They're partners in resilience.

This is the conversation we should be having during International Data Week: how to design systems that are secure by architecture, governed by consent, and transparent by design.

Governance and compliance frameworks mean little if the infrastructure itself isn't trustworthy. Security isn't a checkbox; it's culture, design, and accountability. And those are choices we have to make early and deliberately.

Data Week Lessons: Balancing Protection and Rights

As the world dives deeper into AI-driven data ecosystems, the temptation to "scan everything" will only grow. Proponents will argue that detection equals protection. But International Data Week offers a timely space to ask: protection for whom, and at what cost?

If governments can mandate content scanning under the guise of child protection, what stops future expansions: censoring speech, monitoring journalists, or filtering out whatever's deemed 'unsafe' next.? We've seen how surveillance tools created for one purpose are repurposed for another. The slope isn't theoretical; it's historical.

Germany's stand proves that democratic resistance to overreach is still possible. It also highlights the power of coalition – activists, technologists, journalists, legislators, and everyday citizens working together to hold the line.

That's governance in action: not just writing policy, but living its values.

The Bigger Picture: A Model for Data Ethics

What International Data Week attendees can take from this is a renewed sense of alignment between ethics, engineering, and enforcement.

- **Ethics:** Privacy and protection must coexist; it's lazy governance to claim we can only have one.
- **Engineering:** Encryption, zero-knowledge architecture, and secure data sharing aren't idealistic – they're achievable, proven, and essential.
- **Enforcement:** Data laws must serve citizens, not control them. Oversight, transparency, and technical integrity should be non-negotiable.

Germany's decision wasn't just a legislative act. It was a statement of principle – that we can, and must, protect children without destroying the digital rights of everyone else.

And perhaps that's the broader lesson of International Data Week: good governance isn't about data control; it's about data stewardship.

As data professionals, technologists, and policymakers gather this week, Germany's move offers both inspiration and a warning. If we want a truly safe and equitable digital future, we have to build systems that earn trust, not demand it.

So here's the question worth asking: In our own policies, platforms, and products... are we protecting people, or just managing them?

Kim Chandler McDonald
3 Steps Data Co-Founder/CEO driving data/digital governance solutions | CyAN VP | Multi-award-winning entrepreneur & author

🔓"Pixnapping": when your 2FA codes are stolen pixel by pixel

A previously unknown vulnerability called Pixnapping allows a malicious Android app – without any permission – to steal visual content from other apps (2FA codes, messages, emails) in less than 30 seconds.

💥 **The attack takes place in three key steps:**

- The malicious application invokes the targeted application to force the sensitive information to be rendered on the screen.
- It performs graphical operations on specific pixels.
- It uses an auxiliary channel (linked to the GPU, via a technique similar to GPU.zip) to measure rendering times and reconstruct the content pixel by pixel.

The researchers demonstrated the exploit on Google Pixel and Samsung Electronics GALAXY S25 smartphones, running Android versions 13 to 16. According to the tests, the code recovery rate varies between 29% and 73% depending on the model.

Google has already rolled out a partial fix for Android (CVE-2025-48561), but researchers claim to have bypassed it. A more robust fix is expected by the end of the year.

💡 **Why is this crucial for us?**
This vulnerability calls into question the very foundation of application isolation in Android: a system would want to prevent one application from reading another's screen, but Pixnapping exploits precisely a common rendering mechanism. This threat forces us to reconsider our strategies for visual protection, interface obfuscation, and enhanced isolation of sensitive data.

👉 Protecting against this type of risk requires raising awareness of "visual" risks in mobile environments among DPOs and CISOs. Let's make sure that this type of flaw does not become a vector of choice for attack!

Matthieu Camus
CyAN Board Member, PhD, 10 years of research in AI + 13 years expert in cybersecurity / data protection

The Human Hack Podcast – Mini-Series on Cyberattacks

Featuring CyAN Member Didier Annet

The Human Hack Podcast has launched a new mini-series dedicated to real-world cyberattacks. In the first episode, Didier Annet, CyAN member, expert in cyber-resilience, and certified coach, dissects a cyberattack that hit a Luxembourg company twice in just a few days and brought down its operations.

Didier's calm narration captures the intensity of the crisis while revealing the human dimension behind the technical chaos. With nearly three decades of experience and a background in coaching, he provides a rare dual perspective–combining technical analysis with an understanding of the psychological toll on affected employees.

This episode is based on his work A Guide to Survival of Cyberattacks in Business and Their Psychological Consequences, and sets the stage for two upcoming episodes that will explore the aftermath and perspectives from others involved.

Identity Security Conversations – AI and the Modern Perimeter Featuring CyAN Board Member and APAC Lead Saba Bagheri

In this episode of Identity Security Conversations, host Marco Afzali speaks with Saba Bagheri, CyAN Board Member, APAC Lead, and Cyber Threat Intelligence Manager at Bupa APAC, about how artificial intelligence is reshaping both cyber threats and defense strategies.

Saba explains why identity has become the modern perimeter, outlining how AI-driven attacks are transforming the speed and sophistication of cyber threats. She also shares practical steps for strengthening identity security in financial services, emphasizing the continued importance of multi-factor authentication, awareness of human factors, and threat intelligence in reducing risk.

With over 15 years of cybersecurity experience, Saba provides real-world insights into what defenders face today and how organizations can stay ahead in an evolving threat landscape.

📌 “If you control your identities, you control your risk. If you don’t, attackers will.”

👉 Listen and subscribe for more expert insights via @DelaSecurity.

Cyber (In)Securities | Issue 175

Data Breaches, AI Missteps, and Global Cyber Threats Define This Week's Headlines

This week's issue brings major stories of accountability and awareness. Australian Clinical Labs faces a 5.8 million dollar fine for a data breach affecting more than 220,000 individuals, while Qantas customers voice growing frustration as their personal data surfaces on the dark web. Universities are also under pressure after students were wrongly accused of using AI to cheat, highlighting the human cost of rapid technological change.

Across the globe, hackers exploit F5 devices to target US government networks, MANGO confirms a customer data breach, and Capita agrees to pay 14 million pounds after exposing the information of 6.6 million people.

In our Insights section, we explore how Australians are unknowingly giving away their data, why public Wi-Fi remains a major threat, and how Africa continues to face heavy targeting despite a decline in overall attacks. From Harvard's zero-day incident to the ongoing challenge of balancing modernization with legacy systems, the stories this week underline one truth – cybersecurity is everyone's responsibility.

Voices from the Network

Cybersecurity Advisors Network

The CIA Triad Is Dead – Redefining Trust in Modern Security

From my perspective as a cybersecurity professional in training, the traditional CIA Triad Confidentiality, Integrity, and Availability–no longer captures the complexity of modern digital threats. AI-driven deception, data manipulation, and misinformation have made authenticity and resilience just as critical as encryption or uptime.

The solution lies in evolving toward a trust-centric security model, where technologies such as AI-based phishing detection, zero-trust access, and risk quantification platforms strengthen both prevention and accountability. Tools that integrate governance, data loss prevention, and ESG metrics are redefining how organizations maintain integrity across hybrid systems.

This shift moves cybersecurity from protecting infrastructure to preserving digital trust ensuring the information we depend on remains verifiable, ethical, and transparent in an AI-influenced world.

How to Futureproof IT Teams in the AI Era

As someone deeply interested in cybersecurity and technology governance, I see AI reshaping IT faster than most teams can adapt. Routine monitoring, reporting, and testing are being automated, but the real challenge is ensuring people grow alongside these systems.

To futureproof teams, organizations must invest in AI-assisted tools that enhance learning and decision-making–like intelligent compliance analyzers, automated meeting summarizers, and unified cybersecurity dashboards. Combined with continuous training simulations and real-time performance analytics, these platforms help professionals focus on analysis, risk strategy, and human judgment.

In my view, the future IT workforce will thrive where automation meets awareness where AI handles repetition, and humans lead with adaptability, ethical reasoning, and strategic insight.

Pathan Humam

Current Mentee | Cybersecurity Professional | Penetration Tester | Project Management & Sales Expert | Bridging Technical Solutions with Business Growth

Voices from the Network

CyAN Cybersecurity Advisors Network

The CIA Triad Is Dead – Redefining Trust in Modern Security

The article “The CIA Triad is Dead” by Loris Gutic, while on the surface appearing to merely critique a decades-old model, actually illuminates a recurring theme in cybersecurity: no strategy remains definitive for long. Technology is in a constant state of evolution, and the ways we store, process, and share information are never fixed. As a result, static frameworks like the CIA triad lose relevance, unable to address emerging challenges.

It is naïve to treat past or even present techniques as doctrinal; cybersecurity practices are inherently contemporary, effective only within their specific context and time. To remain resilient, cybersecurity must be adaptive rather than sedentary, continuously evolving alongside the threats and technologies it aims to manage.

Gutic’s proposed improvement to the CIA triad underscores this reality. His layered approach is designed to adapt to emerging technologies, regulatory shifts, and socio-technical dynamics. Just as cyber threats continually mutate, our strategic responses must remain fluid and context based.

Gutic’s article doesn’t merely critique the CIA’s old model; it acknowledges that any framework, both old and new, must be provisional. The article serves as a poignant reminder that, in the field of cybersecurity, resilience lies not in discovering a perfect static framework, but in embracing and designing for ongoing uncertainty.

Isobel McCaffery

Current Mentee | Emerging Cyber Analyst | MQ Security Studies Student | Building Skills in Threat Detection & Analysis

How to Futureproof IT Teams in the AI Era

What struck me most is how the quickly "entry-level" in IT disappearing after AI - and that's not a bad, but it's dangerous if leaders ignore the gap it leaves behind. AI can take over repetitive work, but that work was how people used to learn. It's where future engineers developed problem solving instincts, judgement, and resilience.

Futureproofing IT teams isn't just about teaching people how to use AI tools; it's about rebuilding the ladder entirely. CIOs need to design new was for juniors to gain hands-on experience through mentorship, or simulation based learning. without that, the next generation won't have a chance to live.

AI is forcing IT to evolve fast "and that's healthy" but culture has to evolve with it. The organizations that will thrive are the ones that see learning as an ongoing cycle, not a phase that ends after onboarding.

Efe Zindancı

Current Mentee | Computer Engineer | Aspiring Cybersecurity Professional | SIEM & SIM Internship Experience

Why Signal’s post-quantum makeover is an amazing engineering achievement

Signal Messenger LLC, the subsidiary of the nonprofit Signal Technology Foundation, recently announced a significant set of additions to the Signal Protocol that forms the core of its widely used Messenger platform. Without going into technical detail, the changes consist of major enhancements to the way the protocol generates, exchanges, and manages cryptographic keys, and how it uses these keys to strengthen message encryption. The updates are part of ongoing work to future-proof the Signal Protocol against various forms of attacks using increasingly powerful computational techniques, such as post-quantum cryptanalysis.

While a welcome addition to the strength and credibility of Signal's security and confidentiality, these improvements do not address a major challenge that is not unique to Signal, and that will be difficult to solve technologically. Namely, end-to-end encryption (e2ee) is increasingly under threat by legislative attempts around the world that seek to mandate client-side "backdoors" for law enforcement and intelligence agency access to encrypted messages and other sensitive data. Such mechanisms would grant access to confidential information on end-user devices, where it cannot be protected by encrypted message streams. No matter how strong encryption keys and algorithms are, they cannot protect against your data being accessed in such a manner.

CyAN vehemently and consistently opposes these laws; they threaten the integrity of secure communications, place dissidents and marginalised groups at risk of surveillance, expose personal data to compromise, and undermine trust in secure online commerce and democratic mechanisms. CyAN VP Kim Chandler McDonald published the latest in a series of articles by CyAN members and the Board of Directors expressing our opposition to Chat Control and similar mechanisms that seek to undermine security and privacy with the illusory promise of safety from criminals, terrorists, and other online predators, you can find it here: https://cybersecurityadvisors.network/2025-10-14-germanys-privacy-win-why-it-matters-for-international-data-week/

We recently signed an open letter shared by our partners at the Global Encryption Coalition with European Union member states' ministers on the proposed Regulation on Child Sexual Abuse (CSA), also known as "Chat Control v3". and welcome the apparent failure of this proposal in the face of opposition from Germany and other member states that see it as incompatible not only with personal and societal privacy and secure business online, but also with fundamental digital rights.

Germany's Privacy Win: Why It Matters for International Data Week

Digital governance isn't just about frameworks and policies, it's about people, power, and the principles we're willing to defend when technology overreaches.

READ MORE

John Salomon

vCISO, CyAN board member & startup

Cybersecurity Advisors Network

Australian Clinical Labs fined $5.8m over data breach where 223,000 individuals' personal information was stolen

University wrongly accuses students of using artificial intelligence to cheat

Frustration mounts among Qantas customers as personal data released on dark web

Hackers using F5 devices to target US gov networks

Clothing giant MANGO discloses data breach exposing customer info

YouTube is down worldwide with playback error

Capita to pay £14 million for data breach impacting 6.6 million people

PowerSchool hacker gets sentenced to four years in prison

Fake LastPass, Bitwarden breach alerts lead to PC hijacks

Cybersecurity Advisors Network

China's Flax Typhoon Turns Geo-Mapping Server into a Backdoor

QILIN RANSOMWARE ANNOUNCED NEW VICTIMS

Chinese Threat Group 'Jewelbug' Quietly Infiltrated Russian IT Network for Months

Over 100 VS Code Extensions Exposed Developers to Hidden Supply Chain Risks

ThreatsDay Bulletin: $15B Crypto Bust, Satellite Spying, Billion-Dollar Smishing, Android RATs & More

INSIGHTS

CyAN Cybersecurity Advisors Network

The common way Australians have their data stolen – and what it's costing

Ways CIOs can synergize modernization and legacy infrastructure

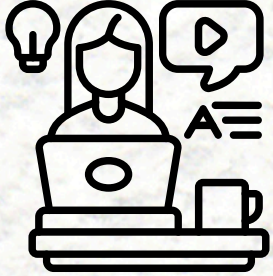
Harvard Is First Confirmed Victim of Oracle EBS Zero-Day Hack

Public wi-fi a major cause of hacking and cyber crime, consumer affairs authorities warn

Africa Remains Top Global Target, Even as Attacks Decline

Editor's Desk

By *Kim Chandler McDonald,*
Editor in Chief



EU need for 'digital sovereignty' is not protectionist, German minister says

When European leaders talk about "digital sovereignty," the term often gets painted as code for protectionism. But as Andreas Rinke's reporting shows, Germany's digital affairs minister is pushing back - arguing that Europe's ambition isn't to wall itself off, but to stand on its own feet. In an era where data is currency and infrastructure is leverage, that distinction matters.

The EU's digital sovereignty push isn't about nationalism; it's about negotiation. Dependence on external cloud providers, chipmakers, and AI platforms has left Europe vulnerable to geopolitical and commercial pressures. Building regional capacity is less about isolation and more aboutensuring that Europe can participate in global digital trade on its own terms - without surrendering control of its data or infrastructure.

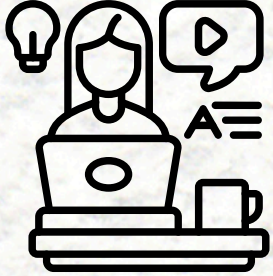
Still, sovereignty isn't something you can declare; it has to be designed. If the EU wants credibility here, its frameworks must remain interoperable, privacy-preserving, and fair. Otherwise, "sovereignty" becomes just another bureaucratic slogan.

For businesses, particularly those outside the bloc, this shift signals a clear direction: data localisation, transparency, and accountability are no longer negotiable add-ons - they're market access requirements.

Europe isn't rejecting the digital future; it's redefining the rules of engagement. And in doing so, it's forcing the rest of the world to confront an uncomfortable but vital question: who really controls the digital foundations we all rely on?

Editor's Desk

By *Kim Chandler McDonald,*
Editor in Chief



Spammers co-opt Google Maps for massive email deluge

We trust what feels familiar. That's why spam arriving through Google Maps doesn't set off alarm bells, at least not right away. When fake reviews and fraudulent listings start driving a flood of deceptive emails, the result isn't just nuisance, it's manipulation by design. A platform built for connection is being turned into a delivery system for deception.

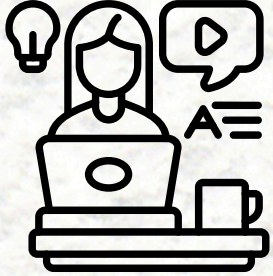
As cybersecurity writer Stuart Corner explains, scammers have learned to exploit the credibility of Google's infrastructure, weaving spam into legitimate notification flows that slip past filters and our own instincts. It's social engineering at its most subtle, using habit and interface familiarity as weapons rather than code.

For businesses, the lesson isn't simply to watch their inboxes. It's to recognise that threat actors are creative system thinkers. They don't need sophisticated exploits when they can manipulate trust loops instead. A compromised reputation can spread faster than a compromised server, and reputation is far harder to patch.

As AI and automation deepen the web of integrations between platforms, these exploit paths will only multiply. Spam filters cannot fix design choices that assume good faith. The smarter response lies in structural defences, tighter authentication, and user control over notification flows. Until that happens, the digital world will remain a map full of traps, and users will keep discovering that not every Google alert points somewhere safe.

Editor's Desk

By *Kim Chandler McDonald,*
Editor in Chief



Hackers leak Qantas data containing 5 million customer records after ransom deadline passes

When five million customer records from Qantas end up online, it's not just a breach... it's a breaking point. Cait Kelly's coverage captures more than just another headline in a long list of ransomware stories; it highlights a systemic fatigue that's setting in across industries. Each new disclosure lands with less shock, not because the threat has lessened, but because the public has become numb to the scale of exposure.

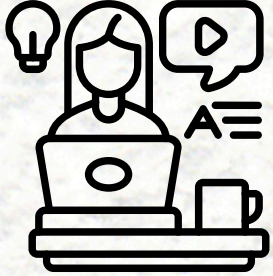
That complacency is dangerous. The airline has long branded itself as a symbol of trust and reliability; when a company such as Qantas falters, the fallout ripples beyond aviation. Travellers, employees, and partners now have to question what personal data means in an economy where even the most well-resourced organisations can't keep it safe.

The airline's response will matter, but so too will the government's. If national carriers are critical infrastructure, then cybersecurity must be treated as safety - not PR management. Transparent disclosure, real-time auditability, and resilient data design must replace platitudes about "lessons learned."

Breaches like this should remind us that privacy isn't just a compliance checkbox - it's part of the social contract between business and customer. When that contract breaks, so does trust. And trust, unlike data, can't be easily restored from backup.

Editor's Desk

By *Kim Chandler McDonald,*
Editor in Chief



Power-hungry data centres threaten Australia's energy grid

Australia's push to become a data hub is colliding with the limits of its own infrastructure. Data centres are consuming more electricity than the grid can comfortably supply, turning digital expansion into an energy liability. The problem isn't just about megawatts, it's about misplaced priorities in how we build and secure our digital future.

Behind every "cloud" pitch lies an industrial-scale consumer of water, power, and risk. When one region holds concentrated digital and energy infrastructure, it doesn't just create an environmental strain – it becomes a single point of failure. Every outage can cascade into both a supply crisis and a cybersecurity exposure.

As InnovationAus reports, governments are being forced to balance data sovereignty, sustainability, and resilience all at once. That balance demands stronger governance linking energy policy and data strategy as twin pillars of national security. Decarbonisation goals mean little if the systems powering them are fragile, over-centralised, or unprotected.

Australia can lead by example, building an energy-aware, cyber-resilient digital economy that's sustainable by intent, not apology. That means transparency in power use, incentives for efficiency and security innovation, and renewable offsets that are real, not rhetorical.

The digital age shouldn't drain the systems that sustain it. If we can't balance energy, security, and innovation now, we risk trading one form of vulnerability for another – and neither will keep the lights on.

Root Access

By *Michael McDonald, APAC*

New Rust-Based Malware "ChaosBot" Uses Discord Channels to Control Victims' PCs

Rust was supposed to make software safer. Now it's making malware smarter. ChaosBot, as reported by The Hacker News, is a new strain of Rust-based malware that uses Discord as its command hub, hiding inside chat traffic that looks completely legitimate. It's efficient, modular, and disturbingly easy to deploy - a clear sign that attacker innovation now mirrors developer progress.

This tactic works because it exploits trust, not code. Discord was built for communication, not containment, and its encrypted APIs make malicious activity blend seamlessly with normal collaboration. The result is a social form of malware that moves with users rather than against them, thriving in the same digital spaces designed for connection.

Security teams need to stop treating language choice or platform reputation as security boundaries. Rust isn't immune to misuse, and Discord isn't a fringe platform. Both sit at the heart of modern digital workflows, which means defenders must expect adversaries to operate there too.

The larger issue is one of misplaced trust. Modern security architectures still assume that collaboration platforms are neutral zones, yet these environments now carry the same attack potential as exposed servers or misconfigured APIs. Treating them as anything less is a strategic blind spot. ChaosBot proves that defenders don't just need better detection tools - they need to start securing the trust layer itself.

Root Access

By *Michael McDonald, APAC*

Hackers Turn Velociraptor DFIR Tool Into Weapon in LockBit Ransomware Attacks

The weaponisation of defensive tools isn't new, but it's accelerating - and the misuse of Velociraptor in recent LockBit campaigns is a textbook example. Ravie Lakshmanan's reportunderscores how open-source forensic tools, designed for transparency and community trust, are being twisted into instruments of intrusion.

Velociraptor is a powerful digital forensics and incident response (DFIR) platform. Its visibility into system artefacts makes it invaluable to defenders and, equally, attractive to attackers who understand its capabilities. By co-opting it, LockBit's operators have effectively blurred the line between forensic analysis and active exploitation, turning defenders' own methodologies against them.

This isn't just a technical issue; it's a governance one. The security community often champions open-source as a trust signal, but open doesn't mean invulnerable. We need to stop assuming intent is self-evident just because code is public. Without stronger provenance checks, usage controls, and telemetry safeguards, open-source tools risk becoming the next unintentional supply chain.

The irony is sharp: defenders built Velociraptor to hunt intruders. Now the intruders are hunting with it. That inversion should unsettle anyone who still treats "open" as synonymous with "safe."

Key Takeaways

c0c0n 2025 – Cyber in Fintech
By Sapann Harish Talwar, Cybersecurity & Risk Executive

At c0c0n 2025, Sapann Harish Talwar shared important insights on cybersecurity in the fintech sector. He spoke about how shared APIs are the backbone of fintech growth but also expand the attack surface. Many organisations still underestimate the cascading risks that come from weak partner APIs.

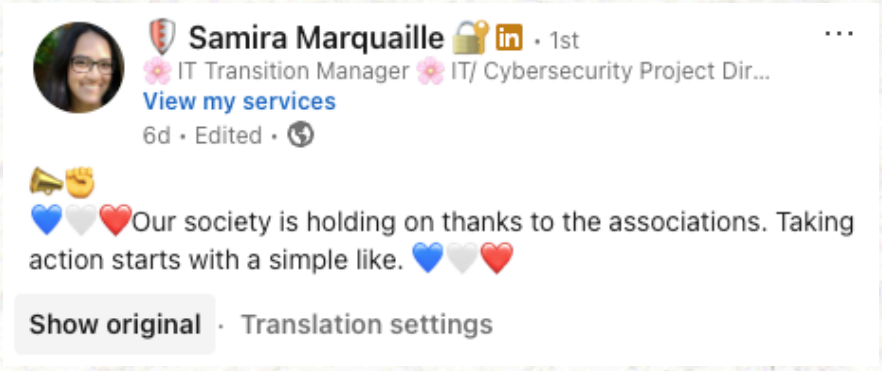
He explained that data sanctity relies on encryption, tokenization, and strict data minimization. A zero trust approach with continuous monitoring ensures that data is used only by the right entities. Immutable logging and reconciliation frameworks help detect tampering at an early stage.

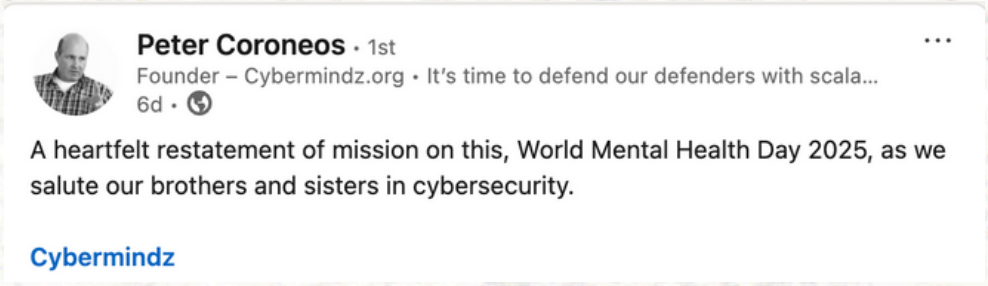
Sapann highlighted that a CISO must begin with risk by design, embedding security due diligence into partner onboarding and technical integration. Continuous API monitoring, third party risk scoring, and data flow mapping are needed to identify hidden interdependencies.

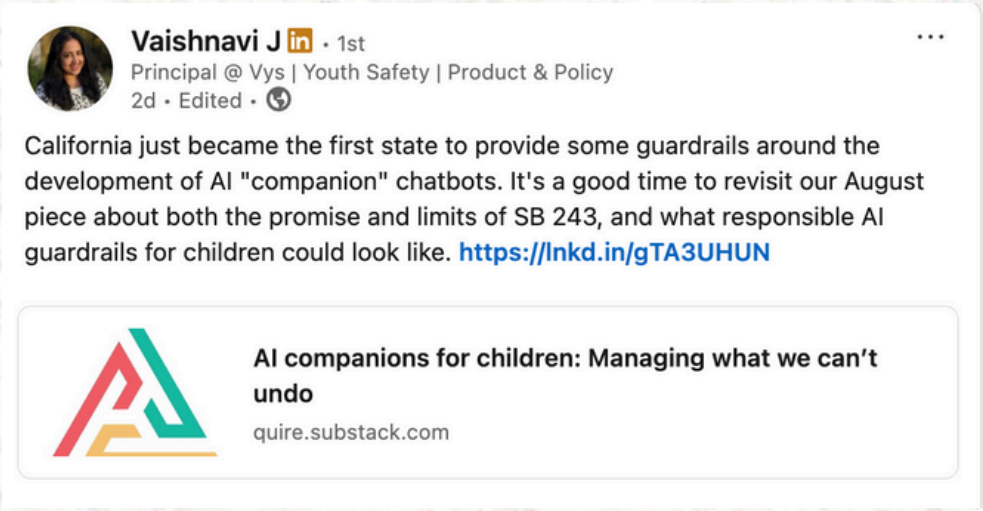
He also stressed that customer consent is necessary, but in today's hyper connected fintech ecosystem, it is not enough. True accountability requires informed consent combined with active protection. Finally, he discussed how RegTech enables supervisors to move from periodic audits to continuous oversight. With advanced analytics, regulators can benchmark compliance maturity, detect systemic risk propagation, and perform what if stress tests. This approach reduces manual oversight burdens and allows regulators to focus on enforcement and resilience planning.

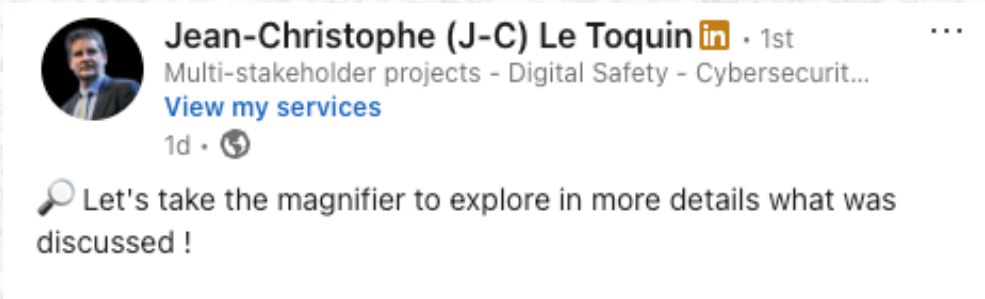
What's On Our Feed

Cybersecurity Advisors Network









Join the conversation by clicking on the image

What's On Our Feed

Cybersecurity Advisors Network

Łukasz Gawron · 1st
CEO #CyberMadeInPoland
3d ·

So what about this cyber sovereignty?

If I had to point to a topic that, from the perspective of the #cyber market in Poland, is the most frequently returned at industry events, I would bet on digital sovereignty. Interesting things heard at conferences and behind the scenes:

Gilles Chevillon · 1st
Operational Resilience, Cybersecurity & Financial Crime | Digital Learnin...
1d ·

Beyond Automation: Agentic AI

Automation is nice. But what compliance really needs is autonomous reasoning.

The Shift We're Living

Most GRC tools record risks and controls. They log data — but they don't think.

Compliance teams still have to connect the dots manually: interpret obligations, review documents, identify gaps, and draft remediation.
It's repetitive, heavy, and slow.

Andrew Pedroso · 1st
APAC Customer Growth & Partnerships @ SoSafe | Human Risk Manage...
1d · Edited ·

An excellent way to kick-off #CyberCon week with a studio recording at Ticker HQ with Jacqueline Jayne! For those attending the conference, feel free to say hi to the ANZ SoSafe team over the coming days to discuss all things security awareness, human risk management, phishing, and the beautiful world of AI.

Join the conversation by clicking on the image

What's On Our Feed

Cybersecurity Advisors Network

Inssata DIOMANDE-RICOURT · 1st
Advisor and speaker in Cybersecurity -Data--Cloud-Transitional CISO & ...
Visit my website
1d ·

#Finance #RiskManagement #Stage #MarchésFinanciers #JeunesTalents #AssetsManagement

Dear Network,
I share the request of Mr. **Abdoulaye hottmann B.**, currently a finance student looking for an internship in financial market risk analysis and financial asset management.

Motivated, rigorous and passionate about financial risk management, he wants to join a bank, management company, fintech or consulting firm to put his skills into practice.

Available from April 2026 for a period of 4 to 6 months.

Any lead or connection will be welcome!

Thank you in advance for your support and sharing 🙏

Join the conversation by clicking on the image

UPCOMING EVENTS

CyAN Cybersecurity Advisors Network

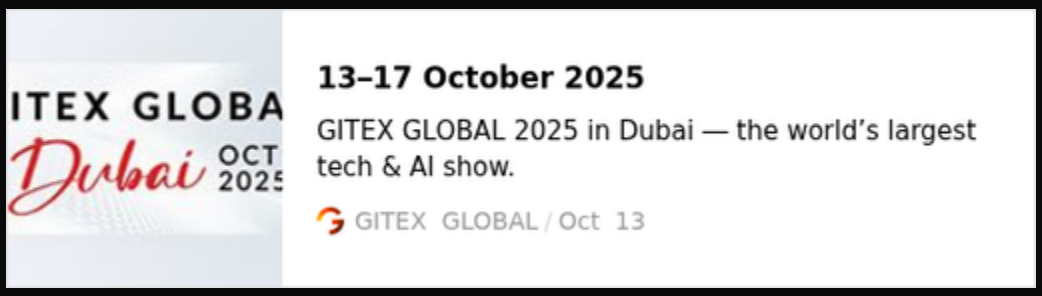
CyAN Cybersecurity Advisors Network

GITEX GLOBAL

13-17 OCT 2025
DUBAI WORLD TRADE CENTRE

THE WORLD'S LARGEST TECH, AI & STARTUP SHOW

COMMUNITY PARTNER



REGISTER NOW

UPCOMING CyAN and CyAN Partner EVENTS:

CyAN APAC Event Series

Nov. 12th 2025
&
Feb. 18th 2026

Details Coming Soon - Save the Dates!

We're delighted to share that Cybersecurity Advisors Network (CyAN) is joining as a partner of the upcoming Third Party & Supply Chain Cyber Security Summit (SCCS), taking place on 4–5 February 2026 in Dubai, UAE.

This summit will bring together global leaders to tackle the complex challenges of supplychainsecurity, tprm, and evolving cyberrisks. As a global, not-for-profit trust network, CyAN is proud to contribute our community's expertise in cybersecurity, privacy, law, forensics, trust&safety, and beyond to strengthen resilience across industries.

🤝 **Partnerships like this help us expand opportunities for collaboration, knowledge-sharing, and impact.**

Special thanks to Bharat Raigangar for making this partnership possible. If you're interested in learning more about CyAN or exploring how to get involved, connect with him directly.

WAM WORLD ADVANCED MANUFACTURING & LOGISTICS Saudi

CyAN Cybersecurity Advisors Network

WHERE MANUFACTURING, LOGISTICS & INNOVATION MEET

SAUDI ARABIA, 15-17 FEB 2026

Register to visit

Book your space

CyAN Returns as a Community Partner for GISEC GLOBAL 2026

We're proud to share that CyAN is once again a Community Partner for GISEC GLOBAL 2026, **the Middle East and Africa's largest AI-Cyber event.** Taking place from **5–7 May 2026** at the **Dubai Exhibition Centre (DEC)**, Expo City, Dubai, GISEC GLOBAL unites over 25,000 cybersecurity professionals from across 180+ countries for three days of collaboration, innovation, and live cyber drills.

Special thanks to Bharat Raigangar for making this partnership possible and for continuing to strengthen CyAN's presence and impact across the MEA cybersecurity community.

GET FREE VISITOR PASS

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!

Follow -US-

YouTube

CyAN Cybersecurity Advisors Network

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

#ReallyInterestingCyberStuff!
#SharingIsCaring