May 24, 2022

Challenge yourself with our Cyber Security Superhero quiz!

This past week's stories:

- Banning Huawei, ZTE won't address all 5G security vulnerabilities, experts warn
- How do Canadian CISOs deal with cyber attacks?
- Safe or unsafe? The cloud's burning cybersecurity question
- Denmark ups cyber security threat level
- IOTW: Costa Rica embroiled in severe, ongoing cyber-attack
- Researchers find a new way to execute malware even while the iPhone is switched off
- Ransomware gangs rely more on weaponizing vulnerabilities
- Data breach attacks costing SMEs without cyber insurance policies thousands each year
- Another arrow in the quiver: Mastercard strengthens cybersecurity consulting practice with new Cyber Front threat simulation platform
- Cybersecurity risk management – 6 best practices
- IP and cybersecurity disputes are top legal concerns for tech companies
- Cybersecurity tips for a safer vacation

Banning Huawei, ZTE won't address all 5G security vulnerabilities, experts warn

Canada needs to focus much more vigilantly on boosting the defence of its 5G wireless network after banning Huawei and ZTE, experts warn, as the country is far behind in cybersecurity.

Thursday's announcement that Canada would bar the Chinese telecom giants from the network came with a promise of speedy legislation to protect critical infrastructure from cyber attacks. That legislation must come with regulations and forward-looking actions that the bans do not address, researchers say.

https://globalnews.ca/news/8852989/huawei-zte-ban-5g-canada-security/

Click above link to read more.

Back to top

How do Canadian CISOs deal with cyber attacks?

The spate of high-profile ransomware incidents in recent years has chief information security officers (CISO) all across the globe alarmed, and a new survey has found that CISOs are now prioritizing preventing such cyber incidents from happening over simply detecting and responding to malware as they happen.

Cybersecurity company Proofpoint surveyed 1,400 CISOs from across the world to prepare its "2022 Voice of the CISO Report." The report looks into how CISOs are adjusting to the pandemic, how they are adapting strategies to support long-term hybrid setups, their changing role as risk demands evolve, and what part people play in the security of their companies.

https://www.insurancebusinessmag.com/ca/news/breaking-news/how-do-canadian-cisos-deal-with-cyberattacks-406660.aspx

Back to top

Safe or unsafe? The cloud's burning cybersecurity question

Last December, Amazon Web Services (AWS)—the world's largest cloud provider, responsible for 40 per cent of global cloud infrastructure in 2021—reported its third outage that month. Previously, a service disruption from AWS wreaked temporary havoc on the digital economy, as companies that rent AWS's cloud servers, such as workplace communication platform Slack, video game developer Epic Games and Amazon's Ring doorbell system, were all forced offline.

Was the source of the problem hackers from far away countries or malicious malware? No. The problem stemmed from a power outage at one of AWS's data centres. Previous outages, which lasted anywhere from one to five hours, were attributed to network congestion and an internal engineering oversight.

https://www.cpacanada.ca/en/news/pivot-magazine/2022-05-18-cloud-security

Click above link to read more.

Back to top

Denmark ups cyber security threat level

Due to increased pro-Russian cyber activity against western European NATO countries recently, the Centre for Cyber Security (CFCS) has upped the cyber security threat level today.

CFCS has increased the threat level from Low to Moderate based on developments in recent weeks brought about by the ongoing War in Ukraine.

https://cphpost.dk/?p=133920

Click above link to read more.

Back to top

IOTW: Costa Rica embroiled in severe, ongoing cyber-attack

Costa Rica's newly elected president, Rodrigo Chaves, declared a state of emergency on 8 May following a month of devastating ransomware attacks carried out by the Conti ransomware gang.

The gang has infiltrated Costa Rican government systems and is holding data to ransom. Originally the ransom stood at $10mn but has recently increased to $20mn.

https://www.cshub.com/attacks/news/iotw-costa-rica-embroiled-in-severe-ongoing-cyber-attack

Click above link to read more.

Back to top

Researchers find a new way to execute malware even while the iPhone is switched off

The iPhone does not completely shut down when you turn it off because it is not completely powered down. Researchers have devised a new kind of malware that can run even when the phone's power is not on. This new type of malware was spotted by researchers at the Technical University of Darmstadt.

It is possible to find a lost or stolen device using the chips that are on the device, which run in a low-power mode during this time. When there is no battery left on an iPhone, the Find My feature can be used, or a credit card and car keys can be used to locate the device.

https://cybersecuritynews.com/execute-malware-iphone/

Click above link to read more.

Back to top

Ransomware gangs rely more on weaponizing vulnerabilities

Security researchers are warning that external remote access services continue to be the main vector for ransomware gangs to breach company networks but there's a notable uptick in exploiting vulnerabilities.

Along with phishing and exploiting vulnerabilities in a public-facing application, these are the primary methods of compromise that ultimately lead to threat actors stealing data and encrypting systems.

https://www.bleepingcomputer.com/news/security/ransomware-gangs-rely-more-on-weaponizing-vulnerabilities/

Click above link to read more.

Back to top

Data breach attacks costing SMEs without cyber insurance policies thousands each year

Small businesses across the UK are counting the cost of not having insurance policies protecting them against the increasing risks of cyber attacks or data breaches.

As small or medium sized enterprises (SMEs) are being targeted by cyber criminals because more employees are working from home, companies across the country are thousands of pounds out of pocket by not having cybersecurity insurance cover.

Figures from the UK Gov Cyber Security Breaches Survey 2022 showed that 39% of SMEs reported cyber breaches or attacks in the space of 12 months, with the average cost of the breaches estimated at £4,200.

https://scottishbusinessnews.net/category/sectors/technology/

Click above link to read more.

Back to top

Another arrow in the quiver: Mastercard strengthens cybersecurity consulting practice with new Cyber Front threat simulation platform

To help customers strengthen their cyber resilience, Mastercard has invested in risk quantification, always-on security monitoring and fraud prevention in recent years

With global cybercrime expected to cost $10.5 trillion USD annually by 2025, innovating cybersecurity remains critical across industries facing rapid digitization. Today, Mastercard announced the launch of new attack simulation and assessment platform Cyber Front, enabled by a strategic minority investment in Picus Security. The tool will help businesses and governments enhance their cybersecurity operational resilience as part of Mastercard's growing Cybersecurity & Risk consulting practice.

https://www.mastercard.com/news/press/2022/may/another-arrow-in-the-quiver-mastercard-strengthens-cybersecurity-consulting-practice-with-new-cyber-front-threat-simulation-platform/

Click above link to read more.

Back to top

Cybersecurity risk management – 6 best practices

Cybersecurity risk management and best practices are crucial to securing your organization's cybersecurity based on identified risks and vulnerabilities. These risks must be prioritized and addressed systematically with the right technologies and security controls.

Here we look at the best practices for effective cybersecurity risk management.

https://cybersecuritynews.com/cybersecurity-risk-management/

Click above link to read more.

Back to top

IP and cybersecurity disputes are top legal concerns for tech companies

No industry is a stranger to litigation, but for the tech sector, it appears intellectual property (IP) and patent disputes, followed by cybersecurity and data protection issues, are among the top legal matters that keep tech company managers up at night.

According to the 17th Annual Litigation Trends Survey by Norton Rose Fulbright, which surveys hundreds of in-house litigation leaders from global corporations, labor and employment disputes are also high on the list for tech companies.

https://techcrunch.com/2022/05/23/ip-and-cybersecurity-disputes-are-top-legal-concerns-for-tech-companies/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADuEPf7bPABmH2aSS93DLtgZFv_GgXjJ4XlXqHhb7nt76aYV0Jf3kpucnBwms79csC6wc2xxjwiH5X0NUqGheGvXTbAjvDXn_drThhBgLH_-C9-BkeMi7jY9q5-n3zHPrdNH7g-k5y66_JtjcoVzL5l1ie7Oyk6ai7rRwUFlWlZZ

Click above link to read more.

Back to top

Cybersecurity tips for a safer vacation

The beauty of having different climates around the world is that there is always somewhere we can travel for leisure all year round. These are times when we tend to relax and let our guard down. The reality, though, is that cyber crime knows no vacation. Attackers are relentless and are always on the lookout for the easiest path to their next prey. That makes us, vacationers, an attractive target. Part of good cybersecurity training involves telling your employees how to protect themselves outside of the office.

Attackers are looking to steal your data or money, wreak havoc or use you to get intellectual property from your work. With the rising rates of cyberattacks and the impact having progressed to include loss of life, we all have a part to play in the fight against cyber crime. Ensuring that we always perform our due diligence and not fall victim to preventable attacks is a step in the right direction.

https://securityintelligence.com/posts/securing-your-trip-safer-holiday/

Click above link to read more.

Back to top