DIRSEC

THE SECURITY SCOOP

QUARTERLY NEWSLETTER | OCTOBER 2024

Industry News

Cyber Insurance: Competition Up, Prices Down

Recent reports reveal a noticeable decline in cyber insurance rates, as competition increases and businesses bolster their security postures. According to a Reuters report, cyber insurance premiums fell in Q2 of 2024 due to improved security practices across industries. Companies that invest in cybersecurity measures, such as multi-factor authentication and employee training, are reaping the benefits of lower premiums, as insurers reward those with proactive defense strategies.

Read More.

In this issue...

Industry News

Energy Companies Ramp Up Cybersecurity Investments

Energy companies are significantly increasing their investments in cybersecurity, particularly as renewable energy sources grow. The industry faces unique challenges due to its reliance on critical infrastructure, which is increasingly targeted by hackers. Companies are now funding startups and investing in technology to close the cybersecurity gap, ensuring that both traditional and renewable energy systems are better protected from cyberattacks.

Read More.

The Rapidly Growing Importance of Cyber Resilience

The July 2024 CrowdStrike incident, resulting in an unexpected outage that affected millions of computers across many industries, reinforced the growing importance of cyber resilience. No organization, not even leading cybersecurity firms, is immune to disruptions. This incident is a reminder that while traditional security measures are essential, businesses must prioritize their ability to anticipate, withstand, and implement effective disaster recovery plans.

Key Takeaways:

- Cyber resilience goes beyond prevention and focuses on quick recovery and adaptation.
- Businesses with strong incident response plans and recovery strategies minimize downtime and losses.
- Core elements of resilience include preparedness, response, recovery, adaptability, and communication.
- Outages and incidents like this highlight the critical need for robust incident response planning.

Click here to learn more about the importance of cyber resilience and how your business can stay prepared for cyber incidents.

Strategic Partnership - DirSec & Summit Security Group

DirSec has partnered with Summit Security Group to enhance its cybersecurity offerings by providing advanced penetration testing services. As cyberattacks grow in frequency and complexity, organizations must identify and address vulnerabilities proactively. The partnership aims to equip businesses with the necessary tools to defend against security breaches through a robust suite of penetration testing options, including network, application, and wireless testing.

Penetration testing, often referred to as ethical hacking, simulates cyberattacks to uncover vulnerabilities in systems, networks, or applications. Summit's expert team conducts thorough assessments to evaluate clients' defenses and recommend effective remediation strategies. This proactive approach not only helps businesses comply with industry regulations but also protects their reputations and assets.

Read More.

Black Hat Recap - Las Vegas 2024

Black Hat 2024, held in Las Vegas, focused on key cybersecurity issues, emphasizing the dual role of artificial intelligence (AI) and machine learning (ML) in enhancing security while also empowering attackers. Experts highlighted the need for organizations to adopt Zero Trust architecture as traditional network boundaries dissolve.

Discussions also covered supply chain vulnerabilities, evolving penetration testing methods, and the persistent threat of organized ransomware. Attendees were urged to enhance incident response plans and invest in security education to reduce human error. Additionally, the importance of research into post-quantum cryptography was underscored, reinforcing the need for collaboration and continuous learning for a secure digital future. **Click here to learn more on the highlights of Black Hat 2024!**

Technology Leaders - Acquisitions

Mimecast - Code42 & Aware Acquisitions

In a move to bolster its AI-powered human risk management capabilities, Mimecast has acquired Code42 and Aware. This acquisition allows Mimecast to expand its portfolio by addressing insider threats and enhancing its ability to protect against human risk factors. As insider threats become more prevalent, Mimecast is positioning itself as a leader in AI-driven risk management solutions.

Read more.

Check Point to Acquire Cyberint

Check Point Software Technologies is set to acquire Cyberint, expanding its threat intelligence and attack surface management capabilities. This acquisition will strengthen Check Point's ability to offer advanced protection against cyber threats targeting businesses globally. The deal underscores the growing importance of attack surface management in an increasingly digital world.

Read more.

ZScaler Acquires Avalor

Zscaler has acquired Israeli startup Avalor for $350 million to enhance its cybersecurity offerings. Avalor's "Data Fabric for Security" aggregates and correlates security data to improve continuous risk management. This acquisition boosts Zscaler's Zero Trust Exchange with better AI-powered vulnerability detection and threat prevention. It will also help automate security operations, using AI to predict breaches and prioritize risks. This aligns with Zscaler's ongoing strategy to strengthen its cloud security through targeted acquisitions.

Read More.

Government Regulations & Federal Cybersecurity News

Healthcare Cybersecurity Act Introduced to Senate

In response to rising cyber threats targeting the healthcare sector, U.S. Senators have introduced the Healthcare Cybersecurity Act. This proposed legislation aims to strengthen cybersecurity defenses in the healthcare industry, which has become a frequent target of ransomware and other malicious attacks. The bill would provide healthcare organizations with the tools and resources needed to safeguard patient data and protect critical infrastructure.

Read More.

FCC Launches Cybersecurity Program for K-12 Schools

The **FCC** is opening up funding opportunities for K-12 schools and libraries to enhance their cybersecurity defenses. This initiative is part of a larger pilot program aimed at improving the resilience of educational institutions, which have seen an uptick in cyberattacks. Schools can apply for funding to upgrade their defenses, providing much-needed resources in an era of growing cyber risks to the education sector.

Read More.

FAA Proposes New Cybersecurity Regulations for Aircraft

The Federal Aviation Administration (FAA) has proposed new cybersecurity regulations designed to address vulnerabilities in aircraft systems. These rules aim to enhance the security of onboard systems and ensure that the aviation industry is better equipped to handle potential cyber threats. As digital transformation continues to permeate the aviation sector, the FAA is looking to close critical gaps in cybersecurity.

Read More.

DIRSEC

THE SECURITY SCOOP

Thanks for reading!

Sign up for our mailing list to receive our quarterly industry newsletters and be the first to know about upcoming events!

Visit **www.dirsec.com/newsletter** to sign up, or reach out to **info@dirsec.com!**

www.dirsec.com

info@dirsec.com

/dirsec