ecosystm.

Securing the Future: Cyber Resiliency in the Digital World

SEPTEMBER 2023

Cyber threats are growing in volume, intensity, and complexity and are here to stay. Basic endpoint attacks are becoming intricate, multi-stage operations. Cybercriminals are launching highly coordinated and advanced attacks. This evolving threat landscape affects businesses of all sizes, jeopardising data, operations, and finances.

> **In the face of massive data leaks, costly ransomware payments, and an ever-expanding and complex threat landscape, the need to strengthen digital defences has driven significant advancements in cybersecurity.**

Critical Cybersecurity Threats

Companies face increased cyberattack risks due to their extensive use of digital technology in daily operations. These attacks, targeting crucial information and infrastructure, are also growing in sophistication.

01 **Data breaches and loss**

02 **Cloud vulnerabilities**

03 **Botnet attacks**

04 **Social engineering attacks on 3rd parties**

05 **API vulnerabilities**

06 **DDoS**

07 **Compromised endpoints**

08 **Credential stuffing**

Challenges That Need to be Overcome

42%

Understanding of the relevant compliance environment

36%

Detecting and managing third party risk

36%

Low cybersecurity awareness in employees and leadership

36%

Accurate assessment of cybersecurity posture and risk

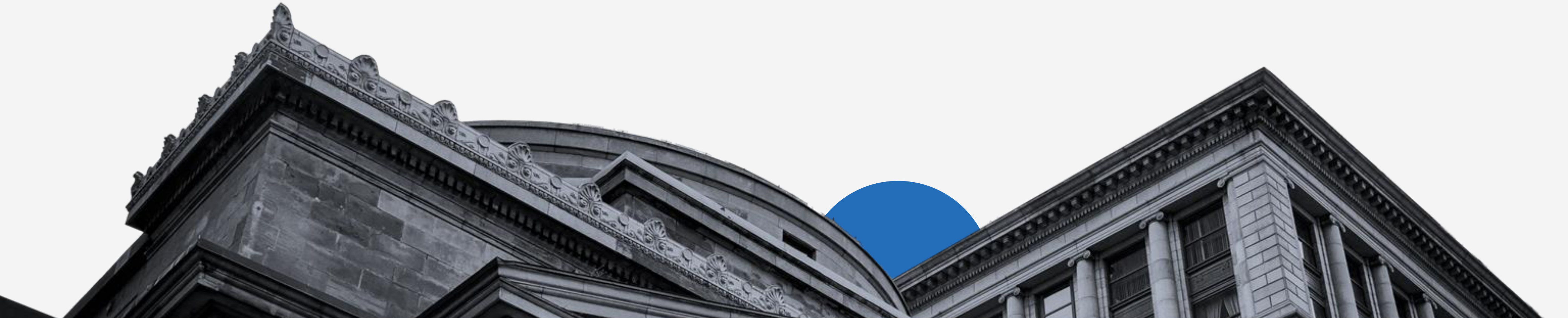
To address the evolving threats and challenges, organisations, governments, industry associations and technology providers are evolving ways to combat cybercrime.

Government Initiatives on the Rise

Global policymakers are implementing stringent regulations, forging global collaborations, and investing in ways to safeguard critical infrastructure and promote resiliency.

New Zealand is creating a central agency to help the public and businesses during network intrusions. The merging of the Computer Emergency Response Team with the National Cyber Security Centre is aimed at better incident response. The rise in online breaches in New Zealand has prompted proactive steps such as gathering financial data related to cyber incidents to better understand and assess cyber risks in the financial sector.

Securities and Exchange Board of India (SEBI) **issued a set of cybersecurity guidelines** to strengthen the cyber security and resilience framework of market infrastructure institutions (MIIs) like stock exchanges, clearing corporations, and depositories. This is incorporated within their operational risk management, given their critical role in trading, clearing, and settlement in the securities market.



Cyber Collaboration Becoming a Reality

Cross-sector collaboration can revolutionise the fight against cyber threats, and stakeholders are realising that.

Taiwan is collaborating with the European Parliament's Foreign Affairs Committee to enhance digital resilience, secure emergency communication using satellite technology, and strengthen defenses against cyber threats. The aim is to promote knowledge sharing and develop robust security frameworks for both countries.

The **Network Resilience Coalition** was founded by cybersecurity leaders across the globe to improve the security of global data and networks. Member organisations such as AT&T, Cisco, and Intel have been working to create actionable recommendations for improving network resilience.

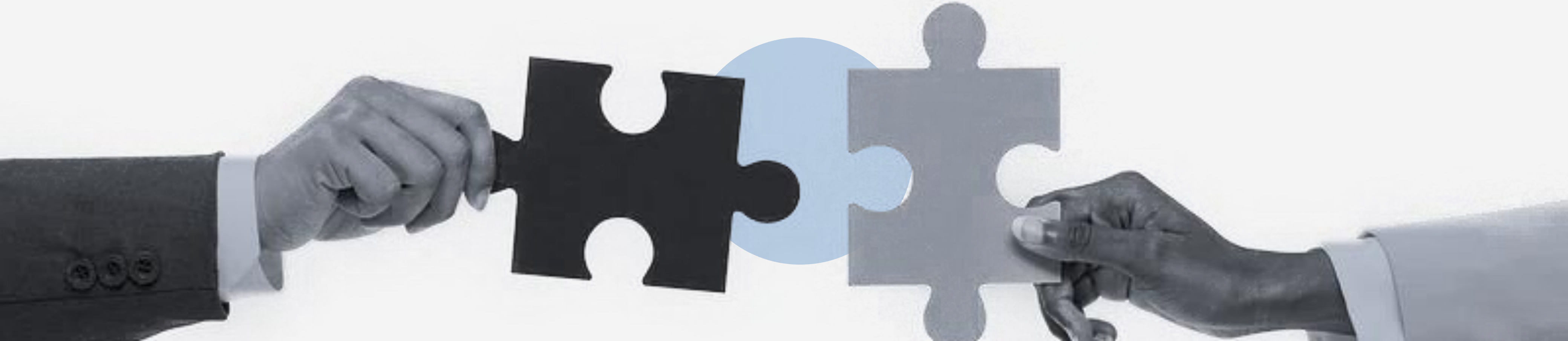
Addressing Vulnerabilities in Operational Technology

Safeguarding critical infrastructure and systems begins with addressing vulnerabilities in operational technology (OT).

Taiwan has introduced cybersecurity requirements for specific IoT devices to safeguard user privacy and IoT network integrity, reflecting global best practices.

The "US Cyber Trust Mark" program was **launched to certify and label IoT devices** like baby monitors and alarm systems with robust cybersecurity. Companies like Logitech and Amazon are backing this initiative to enhance cybersecurity in their product offerings.

Singapore's Cyber Security Agency is working to **boost defences against OT cyber threats**. The initiative involves sharing of threat intelligence sharing, risk assessments, and OT cybersecurity training.



Enhancing Cyber Awareness

Cybersecurity leaders are grappling with the challenge of raising employee awareness about cyber threats.

The **Department of Information and Communication Technology (DICT) in the Philippines** is taking significant steps to establish itself as a cybersecurity hub. This includes workforce training for the IT-BPM sector, forging partnerships with the private sector, and implementing certification programs for students.

Google Cloud is partnering with CERT-In, Indian government's cybersecurity unit, to train 1,000 government officials and offer 100,000 cybersecurity certificate scholarships. This initiative is aimed at boosting cyber skills and Generative AI knowledge among government personnel.

ecosystm.

For more Ecosystm Insights, visit

info@ecosystm360.com

www.ecosystm.io