RANSOMWARE RESILIENCE 2026

Preparing For the Next Generation of Cyber Attacks

19-20 January 2026 | Sheraton Imperial Hotel Kuala Lumpur

Ransomware is one of the most dangerous cybersecurity threats facing organizations globally. The growing frequency and impact of these attacks serve as a stark reminder of the evolving threat landscape and the critical need for organizations to prioritize robust cybersecurity measures to protect their data and mitigate risks.

Ransomware Resilience 2026 Conference returns to Kuala Lumpur for its highly anticipated 2nd edition, where the region's finest cybersecurity minds will gather to share cutting-edge insights, brainstorm solutions, and forge alliances.

Dato' Ts Dr. Haji Amirudin Abdul Wahab
CEO
CYBERSECURITY MALAYSIA

Jason Murrell
Co-Founder
MURFIN GROUP

Chirag Joshi
CISO & Founder
7 RULES CYBER

Jelena Matone
CISO
EUROPEAN INVESTMENT BANK

Abid Adam
Group Chief Risk & Compliance Officer
AXIATA GROUP

Sadeed Tirmizey
CISO
SEQWATER

Brenda Van Rensburg
Cybersecurity GRC & Assurance Head
TERRENE GLOBAL

Lukas Stefanko
Malware Analyst
ESET

Kevin O' Leary
CISO
KYNDRYL

Dr. Sharifah Bahiyah Rahayu
Cyber Security Director
NATIONAL DEFENSE UNIVERSITY, MALAYSIA

Tanvinder Singh
Cyber Security & Privacy Director
PWC MALAYSIA

Peter Mosmans
Founder
GO FORWARD

Indrani Chandrasegaran
Senior Director Technology Advisory
VCYBERIZ

Abhinav Mishra
Founder
ENCIPHERS

Chris Cubbage
Director
MYSECURITY MEDIA

Danish Tariq
Director, Cyber Security
LABURITY

Shahmeer Amir
CEO & Co-Founder
SPEEQR

Hassan Khan Yusufzai
Co-Founder
LABURITY

Book Your Seats: ☎ +603 22606500 🌐 www.cybersecurityasia.tech

Organized by: THOMVELL international

Overview:

In the face of the rapidly evolving and perilous landscape of cybersecurity, **Ransomware Resilience 2026** offers a critical opportunity to stay informed, upskill, and outwit the relentless cybercriminals who relentlessly threaten our digital world.
Cybersecurity is facing a tectonic shift, driven by the unrelenting evolution of ransomware. With the staggering cost of ransomware predicted to reach $265 billion by 2031, organizations must rise to the challenge and adapt to stay ahead of the ever-changing landscape of cybercrime to prepare for the next generation of attacks.

Join Malaysia's Ransomware Resilience 2026 conference to benchmark resilience and business continuity planning, sharing cutting-edge strategies, action plans, and best practices. Empower your business to prevent, detect, and respond effectively to security challenges, ensuring your organization's resilience against the growing threat of cyber extortion.

WHY ATTEND

Prepare for the Future
Get a front-row seat to the latest advances in ransomware defence, detection, and response strategies

Anticipate Evolving Threats
Learn about emerging attack vectors and countermeasures to stay one-step ahead of the ransomware menace

Harness Expert Insights
Hear from the industry's top thought leaders, practitioners, and researchers who are shaping the future of ransomware resilience

Reach key Decision-Makers
Connect with a highly targeted audience of senior cybersecurity professionals who are actively seeking solutions to mitigate ransomware threats

Forge Valuable Connections
Network with peers from various industries and sectors to build a community of resilience, exchange best practices, and expand your professional network

Gain Competitive Edge
Join the only national platform covering Ransomware Resilience under one roof, delivering a complete cross-sector perspective on Malaysia's innovation landscape helping businesses to plan, prepare, and recover from a ransomware incident

WHO SHOULD ATTEND

- Chief Executive Officers
- Chief Operating Officers
- Chief Information Security Officers
- Chief Information Officers
- Chief Risk Officers Chief
- Threat Defence Heads
- Incident Response Managers
- Threat Intelligence Heads
- Cyber Crisis Management Heads
- Ransomware Incident Responsive Teams
- Technology Officers
- Cyber Security Professionals
- Heads of Digital Transformation
- Heads of Insights and Analytics
- Operation Risk Heads and Managers
- Technology Risk Heads and Managers
- Cyber Security Experts
- Operational Technology (OT) Cybersecurity
- Global Operational Technology (OT) Cybersecurity

46%

of CSOs and CISOs believe ransomware as their biggest cybersecurity threat

Average financial impact now

$1.85m

and rising

PROGRAM OUTLINE

DAY 01 : 19 January 2026

8:00 - 8:45 AM — **Registration | Morning Refreshments | Exhibition Browsing**

9:00 - 9:35 AM — **Opening Keynote:**

STAYING AHEAD OF RANSOMWARE THREATS: A HOLISTIC APPROACH FOR MALAYSIAN ORGANIZATIONS

Malaysian organizations are increasingly at risk of ransomware attacks, which have become a predominant threat to cybersecurity. Keynote insights will provide a comprehensive view of the current ransomware landscape, with a focus on the emerging tactics and strategies being deployed by cybercriminals. Dato' Amirudin will discuss the key principles of a holistic, proactive approach to ransomware defense, from preventing and detecting attacks, to effectively mitigating damage and responding to breaches.

Dato' Ts Dr. Haji Amirudin Abdul Wahab, *CEO,* **CYBERSECURITY MALAYSIA**

9:40-10:15 AM — **Fireside-Chat: Special Guest**

DRIVING MALAYSIA'S DIGITAL FUTURE FROM CYBERTHREATS TO INNOVATION

This session sheds light on the evolving ransomware threat landscape, presenting recent trends and real-world case studies to underscore the gravity of the issue. Delving into the financial implications of ransomware attacks, it unveils the hidden costs that go beyond ransom payments, urging businesses to take proactive measures. To counter this menace effectively, the session outlines preventive measures that organizations can adopt. In an era when ransomware adversaries continuously evolve their tactics, this session arms businesses with valuable insights and practical strategies to forge a secure future, turning the tide against ransomware and bolstering their resilience in the face of this persistent cyber threat.

Moderator : **Chris Cubbage**, *Executive Director,* **MYSECURITY MEDIA**

10:15-10:45 AM — **Morning Break | Exhibition Browsing**

10:45-11:45 AM — **Stage-Talk**

11:45- 12:30 PM

FROM BREACH FATIGUE TO CYBER FIT CULTURE: TURNING PEOPLE INTO A CONTROL

Most incidents start with human slip ups, not zero days. This session shows how to turn awareness into behaviour change, simple rituals that stick, role-based accountability and 'nudge' design that reduces risky clicks. Jason links culture to identity controls (least privilege, MFA habits) and gives leaders the metrics that prove improvement to boards, regulators and insurers. You'll leave with a 90-day playbook to measure, coach and hardwire safer behaviour at scale.

Jason Murrell, *Co-Founder,* **MURFIN GROUP**

12:30-1:00 PM

IDENTITY SECURITY: NEW THREATS – NEW PARADIGMS

As the threat landscape continues to intensify, relying on traditional models to secure identities is a losing proposition. It's time to challenge conventional thinking and apply new security models to defend against identity-based cyberattacks. In today's world, characterized by the proliferation of identities and the double-edged sword of AI, every organization must embrace a set of new paradigms to secure every user - human and machine.

Jelena Matone, *CISO,* **EUROPEAN INVESTMENT BANK**

1:00-2:00 PM — **Lunch**

2:00-2:40 PM — **Panel Discussion:**

SAFEGUARDING DATA PRIVACY IN THE FACE OF RANSOMWARE

In the age of big data, safeguarding data privacy poses a challenge for businesses and corporations. The threat of ransomware attacks only magnifies this concern. Join us for a compelling discussion as we explore practical strategies to reinforce data privacy pre- and post-incident, along with holistic approaches to strengthen resilience against cyber threats. Discover how organizations' can achieve their privacy and cybersecurity goals without compromising valuable resources.

Moderator : **Dr. Sharifah Bahiyah Rahayu**, *Cyber Security Director,* **NATIONAL DEFENSE UNIVERSITY, MALAYSIA**

Panellist : **Tanvinder Singh**, *Cyber Security & Privacy Director,* **PWC MALAYSIA**
Abid Adam, *Group Chief Risk & Compliance Officer,* **AXIATA GROUP**

2:45-3:10 PM — **Stage-Talk**

3:15-3:45 PM

NGATE: ANDROID MALWARE FOR UNAUTHORIZED ATM WITHRAWALS VIA NFC RELAY

While theoretical NFC relay attacks have been discussed for years, real-world attacks remain rare – especially successful ones. Lukas will delve into NFCGate, the legitimate, open-source, NFC research toolkit that the NGate malware is based on explaining 2 additional attack scenarios that can be achieved using the same tooling. Lukas demonstrates NFC attacks against contactless payments, and NFC token cloning showing how attackers can use a smartphone to scan contactless cards in public places, enabling them to make payments simultaneously at a remote terminal. He will present how an attacker can clone the UID of MIFARE Classic 1k NFC contactless smartcards to gain access to restricted areas plus sharing on crimeware technique that exploits NFC technology to conduct mobile payments worldwide using stolen payment cards and phishing-obtained one-time passcodes.

Lukas Stenfanko, *Malware specialist,* **ESET**

3:45-4:00 PM — **Evening Break | Networking & Exhibition Browsing**

4:10-4:50 PM

RANSOMWARE VS ZERO TRUST: CISO STRATEGIES FOR CYBER RESILIENCE IN THE AI ERA

In today's cybersecurity landscape, ransomware attacks are becoming increasingly sophisticated and complex, challenging traditional security measures. To ensure resilience against these threats, CISOs must adapt their strategies to accommodate the dynamic nature of the digital landscape, including:

- Assessing the viability of zero trust architectures in mitigating ransomware attacks
- Understanding the impact of AI-driven threats and developing countermeasures
- Planning for business continuity and operational resilience in the face of cyber attacks
- Sharing insights and best practices on strengthening cybersecurity frameworks

Kevin O' Leary, *CISO,* **KYNDRYL**

4:50-5:30 PM

ARTIFICIAL INTELLIGENCE DRIVEN RANSOMWARE: ATTACK AND DEFENSE

Artificial Intelligence is now being used by adversaries to perform ransomware attacks that are more deadly than ever. Even though the dirty work of extorting money can vary, the results of encrypting the data is the same. Tools that can quickly scrape data from the internet have been developed thanks to the increasing expansion of AI. At the same time, embedding AI into your cyber defense practice can keep track of behaviour alterations of ransomware that can portend a forthcoming attack & can deal with unprecedented threats. Shahmeer will examine and showcase how AI will revolutionize both the attack and defense against ransomware.

Muhammad Shahmeer Amir, *Ethical Hacker & Co-Founder,* **SPEEQR**

DAY 02 : 20 January 2026

8:00 - 8:45 AM — **Registration | Morning Refreshments | Exhibition Browsing**

9:00 - 9:35 AM — **NAVIGATING RANSOMWARE ATTACKS FROM CHAOS TO RECOVERY**

Are you truly ready to confront a ransomware attack head-on? Have you experienced the devastating aftermath of such incidents?
This captivating presentation will reveal how rapidly ransomware can cripple a business. From Disaster Recovery Plans to Legal Obligations, attendees will witness firsthand why each piece of information, gathered and/or used before and during a ransomware attack, is crucial for a successful recovery. The ultimate goal is to equip participants with knowledge and practical skills that strengthen their organization's cyber defense strategies against constantly evolving ransomware threats.

Brenda Campbell, *Data Protection & AI Governance Head,* **TERRENE GLOBAL**

9:50-10:15 AM — **Stage-Talk**

10:20-10:40 AM — **Morning Break | Exhibition Browsing**

10: 45-11:15 AM — **Stage-Talk**

11:20-12:20 PM — **60-Minute Crisis Simulation:**

EXECUTIVE STRESS TEST: SURVIVING THE RANSOMWARE CRISIS

Ransomware is no longer a technical problem. It is a boardroom crisis that tests leadership, governance and trust. This gamified exercise drops executives into the centre of an unfolding ransomware attack. Participants will confront tough decisions on ransom payment, operational shutdowns, regulatory disclosure and public communication. Each choice carries consequences that shape customer confidence, market stability, and the future of the organisation. This is a stress test for the modern executive: can you guide your company through the crisis and emerge with trust intact?

Chirag Joshi, *Founder & CISO,* **7 RULES CYBER | *President*, ISACA Sydney Chapter**

12:25-1:05 PM — **FROM BREACH TO RECOVERY: BUILDING REAL RANSOMWARE RESILIENCE IN ENTERPRISE**

Ransomware isn't just about stopping the breach—it's about surviving it. In this session, Abhinav Mishra shares real-world insights on breaking the ransomware kill chain and explains how organizations can prevent the majority of attacks by effectively remediating critical and high-severity CVEs across their infrastructure. Since these vulnerabilities are the primary entry points ransomware campaigns exploit, prioritizing their mitigation is one of the most powerful resilience strategies available. The real question is—does your security team know how to identify and remediate CVEs before attackers do?

Abhinav Mishra, *Security Researcher & Founder,* **ENCIPHERS**

1:05-2:00 PM — **Lunch**

2:00-2:40 PM — **Panel Discussion:**

ENDPOINT PROTECTION TO THREAT HUNTING: BUILDING PROACTIVE RANSOMWARE DEFENSES

Learn how to proactively defend your organization against ransomware attacks by hardening networks, reducing vulnerabilities, and stopping ransomware dead in its tracks. This panel will delve into endpoint protection, network segmentation, and the importance of threat hunting to identify and neutralize hidden adversaries.

Moderator : Chris Cubbage, *Executive Editor & Founder,* **MYSECURITY MEDIA**

2:45-3:20 PM — **SECRET SCANNING IN OPEN-SOURCE AT SCALE & PREVENTION: SUPPLY-CHAIN RISK**

Supply chain security conversation is booming these days after attacks like log4j came to the scene. In this in-house research, we have conducted research on publicly available open-source assets like NPM (JS packages) and WordPress Plugins find out the presence of mistakenly or deliberately publicly exposed secrets (including private API keys and so on) i.e. AWS, Google, etc. (33 different categories of secrets!). This could pose a risk to anyone using those packages as dependencies or plugins so that this chain of not reinventing the wheel could become a disaster that stops the wheel once and for all. Speakers demonstrates the numbers & impact to the audience and provide ways to prevent this and automation to integrate in your own ci/cd pipelines to prevent such disasters from happening.

Dannish Tariq, *Director Cyber Security,* **LABURITY**
Hassan Khan Yusufzai, *Director & Co-Founder,* **LABURITY**

3:20-3:40 PM — **Evening Break | Exhibition Browsing**

3:45-4:15 PM — **THE ANTI-AI PARADOX: HOW CHAOS ENGINEERING BEATS RANSOMWARE**

Artificial Intelligence, while powerful, cannot predict or protect against all potential cyber threats. Chaos engineering, on the other hand, empowers organizations to become more resilient in the face of unexpected events, including ransomware attacks. This engaging talk will explain how companies can better deal with cyber security risks, by casually sprinkling chaos into day-to-day processes. AI can improve detection, but it also increases our dependency on systems - systems that might be unavailable during critical times. Peter will show how chaos engineering can be used as a tool against ransomware, revealing weaknesses and vulnerabilities that would otherwise remain hidden.

Peter Mosmans, *Founder,* **GO FORWARD**

4:20-4:45 PM — **AGENTIC AI: THE NEXT FRONTIER OF ADVERSARIAL THREATS**

Agentic AI-AI systems capable of autonomous decision-making-are rapidly being integrated into enterprise workflows. This session explores how agentic AI blurs the lines between traditional cyberattacks and adversarial AI, introduces new attack vectors (such as phishing via agentic systems and local model tampering), and necessitates a new breed of incident response playbooks. Attendees will learn how to proactively test agentic AI for vulnerabilities, develop tailored incident response strategies, and foster resilience against evolving threats.

Indrani Chandrasegaran, *Senior Director, Cyber Advisory & Global Tech Services,* **VCYBERIZ**

4:45-5:20 PM — **Closing Keynote:**

BEYOND RANSOMWARE: BUILDING INCIDENT RESPONSE PREPAREDNESS FOR ICS/OT ENVIRONMENTS

This presentation will explore how organizations can extend traditional IT incident response practices into the ICS/OT domain to strengthen resilience against disruptive cyber events. It will focus on:

- Practical steps to integrate OT/ICS into enterprise response playbooks.
- Facilities, equipment, and personnel readiness for critical operations.
- Communication structures that align incident response with executive crisis management.
- A Preparedness Checklist for participants to benchmark and stress-test their capabilities.

Sadeed Tirmizey, *CISO,* **SEQWATER**

5:20 PM — **Lucky Draw & Conference Closing**

SPEAKER BIOGRAPHY

Dato' Ts. Dr. Haji Amirudin Abdul Wahab is the Chief Executive Officer of CyberSecurity Malaysia, the national cybersecurity specialist and technical agency responsible for safeguarding Malaysia's cyberspace and digital sovereignty. With over 30 years of experience in the ICT industry, Dato' Dr. Amirudin has held key positions across both the public and private sectors, particularly in telecommunications and information technology. He holds a PhD from the University of Queensland, Australia; a Master of Business Administration (MBA) from the University of Dubuque, Iowa, USA; a Master's degree in Information Technology from the National University of Malaysia (UKM); and a Bachelor of Science in Electrical Engineering from the University of Michigan, Ann Arbor, USA. Under his visionary leadership, CyberSecurity Malaysia has achieved significant national milestones and global recognition. Dato' Dr. Amirudin has also served as Chairperson on numerous national and international platforms, advocating for robust cybersecurity strategies and capacity building. He is currently an Adjunct Professor at several institutions of higher learning in Malaysia and was awarded an Honorary Doctorate in Information Technology (Cybersecurity) by Universiti Teknikal Malaysia Melaka (UTeM) in recognition of his contributions to the field. Dato' Dr. Amirudin has received numerous awards and accolades throughout his career. Most recently, he was conferred the National Technologist Award 2024 by the Ministry of Science, Technology and Innovation Malaysia. On 16 October 2024, His Majesty the Yang di-Pertuan Agong appointed him as a Member of the National Anti-Financial Crime Centre (NFCC) Advisory Board. In November 2024, he was also appointed to the Advisory Panel of the Bumiputra Economic Study Institute at University Poly-Tech Malaysia (UPTM).

Kevin O'Leary is the leader of the Security and Resiliency practice at Kyndryl, assisting customers across the region in navigating their cyber risks with confidence, meeting regulatory requirements, and becoming operationally resilient. O'Leary brings over 25 years of extensive experience as a chief information security officer (CISO), cybersecurity subject matter expert, and IT executive. His career includes leadership roles across Asia, Australia, Europe, and the Middle East, working with major multinational companies in industries such as finance, manufacturing, and technology. Before joining Kyndryl, O'Leary served as the APAC Regional CISO and head of Cybersecurity and Technology Controls for JP Morgan. Earlier in his career, he was the field chief security officer for Palo Alto Networks, APJ, where he promoted cybersecurity strategies across Asia Pacific and Japan.

Jelena Matone is a respected and leading CISO at European Investment Bank, who was awarded the CISO of the year for 2019 in Luxembourg, and recently 'CISO Sentinel GLOBAL'. Jelena is a versatile and innovative Cybersecurity professional with emphasis on cyber security risk management, policies and procedures creation, IT/IS security, IT Operations, audit, risk mitigation, business process improvement and IT governance. She is also a member of World Economic Forum, Founding board member and first president of Women4Cyber & Woman Cyber Force. Prior to her current role at EIB, Jelena served as the Senior Operational Risk and ISO for the European Stability Mechanism, the crisis resolution mechanism for euro area countries.

Abid Adam is a recognized leader in Cybersecurity, Data Privacy, Enterprise Risk Management, and Compliance. As the Group Chief Risk & Compliance Officer (GCRCO) at Axiata Group, he has led transformative initiatives across Asia, Africa, and Latin America, driving strategic advancements in these critical areas. Abid's influence extends to global forums, actively contributing to the World Economic Forum's Digital ASEAN initiatives and the Pan ASEAN Data Policy and Cybersecurity Taskforce. His commitment to a secure digital economy is central to his mission of aligning technological growth with robust security measures. In addition to his executive role, Abid served as an adjunct professor at Deakin University, shaping future leaders in cybersecurity. With a background in Computer Science and professional credentials including CISSP, CISM, CRISC, and MBCI, Abid is dedicated to fostering a safer, more secure digital landscape.

Lukas Štefanko is an experienced malware researcher with a strong engineering background and a well-demonstrated focus on Android malware research and security. With more than 13 years' experience with malware, he has been focusing on improving detection mechanisms of Android malware and in the past couple of years has made major strides towards heightening public awareness around mobile threats and app vulnerabilities. He has presented at several security conferences such as RSA, Virus Bulletin, Confidence, DefCamp, BountyCon, AVAR, CARO Workshop, Infoshare, Ekoparty, Code Blue, and Copenhagen CyberCrime.

Abhinav Mishra a.k.a 0ctac0der, is an Application Security Researcher with over 13 years of experience in penetration testing across web, mobile, and infrastructure. He is the founder of ENCIPHERS, leading offensive security projects, including penetration testing, red teaming, and specialized training programs. In addition to his deep expertise in traditional security domains, Abhinav has expanded his focus to AI security, with experience in assessing the robustness of machine learning models, securing AI-powered applications, and researching adversarial attack techniques. He has been actively involved in helping organizations integrate secure AI systems into their existing infrastructure. He holds numerous accolades & rewards for finding security issues through responsible disclosure programs. He is a well-known trainer, speaker, cyber security strategist and ethical hacker in the information security community, where he majorly talks about the offensive security/penetration testing/responsible disclosures/AI Security. He authored the book "Mobile App Reverse Engineering".

Hassan Khan is a highly experienced Security Researcher with a proven track record of internet-wide scanning and penetration testing. A sought-after speaker, Hassan recently presented at the BlackHatMEA 2022, 2023 conference. His expertise extends to Ruby security, where he has conducted extensive research over the past few years. As a certified OSCP, Hassan has made a name for himself as a successful bug bounty hunter on both HackerOne and Bugcrowd. His achievements have earned him recognition in the industry, including inclusion in the Google Security Hall of Fame (2017), Twitter Security Hall of Fame (2017), and Microsoft Security Hall of Fame (2017). He has also conducted extensive research into WordPress security and won the HackFest CTF competition. In addition to his research, Hassan is also the developer of several security testing tools and an npm scanner for account hijacking, further demonstrating his commitment to the security field and his skills as a developer.

Chris Cubbage is Director and Executive Editor for MySecurity Media and principal security consultant with Amlec House. With over 30 years' experience, Chris is a multi-certified security professional with a formative 15 years policing background, including as a Homicide Detective and Australian Crime Commission Senior Investigator. Chris is author of Corporate Security in the Asia Pacific Region, Security Risk Management in Corporate Governance and publisher of Cyber Risk Leaders by Shamane Tan. Chris is host of MySec.TV, Cyber Security Weekly Podcast and editor of the Australian Cyber Security Magazine and Cyber Risk Leaders Magazine.

Peter Mosmans started out in the nineties as a software engineer working on internet banking applications for various European financial institutions. Then he moved to the role of defending and designing systems and networks for high-availability web sites. Since 2004 he started specializing in breaking: pentesting complex and feature-rich web applications. Currently he spends his time on teaching secure coding principles, consulting companies on DevSecOps, and penetration testing.

Jason Murrell is a cyber security strategist, investor and keynote speaker who helps boards, CISOs and founders turn cyber risk into competitive advantage. He is Co-Founder of Murfin Group, former Chair of the Australian Cyber Network (ACN) and current Chair of DSI's SMB1001 security standard. Jason also serves as Entrepreneur in Residence to the AU $100m Fusion the next wave of deep tech scaleups. He has advised government agencies, ASX boards and global technology firms on ransomware response, identity security, privacy regulation and resilience. A repeat founder and early investor across award winning ventures, from consumer brands to cutting edge cyber and AI, Jason blends policy insight, breach war stories and startup pragmatism. He regularly leads executive briefings and publishes industry insight, including the ACN State of the Industry work. Jason's sessions are known for clarity, actionable playbooks and measurable outcomes.

Chirag Joshi is a globally recognised cyber security leader, author, Founder & CISO of 7 Rules Cyber. A multi-award-winning executive, Chirag was named Cyber Security Consultant of the Year at 2025 Australian Cyber Security Awards. He previously received the Excellence Award and has been recognised on the CSO30 list of Australia's top cyber security executives for three consecutive years (2022–2024). Currently Chirag serves as President for ISACA Sydney. Chirag brings global leadership experience across critical infrastructure, financial services, government, energy, healthcare, higher education, consulting, and the not-for-profit sector. He has led major cyber transformation programs, advised boards and executives, and guided organisations through M&A activity, regulatory change, and operational technology risk. In addition, he is the National Ambassador for the Critical Infrastructure ISAC Australia, promoting trusted collaboration, threat intelligence sharing, and enhanced cyber resilience across Australia's most essential sectors.

Indrani Chandrasegaran is the Senior Director of Consulting and Technology Advisory, APAC at vCyberiz and a transformative cybersecurity leader with over 24 years of global experience driving AI-powered resilience, enterprise risk strategies, and board-level cyber governance. She has held executive leadership roles at EY, Accenture, Infosys Compaz, Trusted Source (Temasek), and Symantec, where she led multimillion-dollar cybersecurity transformations across APAC, the Middle East, and Europe. A recognized thought leader, she advises boards and C-suites on navigating complex cyber threats, regulatory challenges, and the responsible adoption of emerging technologies. Her expertise spans cyber strategy, AI-driven defense, MSSP development, partner ecosystems, and resilience-by-design programs that enhance business continuity and operational excellence. She has been honored as one of the Top 20 Cyber Women in Singapore, Top 30 in ASEAN, and DRII Cyber Program Leader of the Year, and serves on advisory boards for renowned global technology companies.

Sadeed Tirmizey is a seasoned cyber security leader with over 20 years of experience across the industry. He's held senior roles at Airservices Australia, Queensland Health, and is currently the CISO at Seqwater. Sadeed is known for building high-performing security programs that support business goals, not slow them down. He brings a strong focus on strategy, risk, and culture - making cyber a partner in growth, not just a gatekeeper. In his words: 'Cyber shouldn't slow you down - it should keep you in business.'

Brenda van Rensburg is a recognized authority at the intersection of data, security, and artificial intelligence. With a Bachelor of Science, a law degree, and postgraduate qualifications in AI, she brings a rare blend of technical and legal expertise to the evolving landscape of cybersecurity and governance. Brenda's career spans sectors as diverse as mining, insurance, finance and government, giving her a well-rounded view of risk and resilience across industries. Currently she works in P & N Bank based in Perth Australia. As an international speaker and author, she will share a critical message on how quickly ransomware can cripple a business; highlighting the implications from disaster recovery to legal accountability in a hyper-connected world.

Shahmeer Amir s a globally recognized Cyber Security Entrepreneur and Ethical Hacker; was awarded Entrepreneur of the year 2024 for founding multiple startups including Speeqr plus ranking as the third most accomplished bug hunter globally. He spoke at over 130 conferences worldwide and his expertise has been instrumental in assisting 400+ Fortune companies, such as Facebook, Microsoft, Yahoo, and Twitter, in resolving critical security issues within their systems. Shahmeer's entrepreneurial ventures in the technology realm have led to the establishment of multiple startups, with his current role involving the leadership of Speeqr, and involvement in Veiliux and Authiun. He serves as the Cyber Security Advisor to the Ministry of Finance in the Government of Pakistan. His involvement spans various projects, including Deep Sea Tracking, Digital Transformation of Legislation, and the Digitization of Pakistani Cultural Content. As a testament to his influence in the tech industry, he holds a position on the Forbes Technology Council.

Danish Tariq is a Security Engineer by profession and a Security researcher by passion. He has been working in Cyber Security for over 8 years and it all started out of a curiosity to break things and look deep down into those things (physical or virtual) back in his teenage years. His major expertise is Penetration Testing and Vulnerability Assessments. He was also involved in bug bounty programs as well, where he helped many companies by finding vulnerabilities at different levels. Companies include Microsoft, Apple, Nokia, Blackberry, Adobe, etc. He spoke at Blackhat MEA and was featured in "The Register" for an initial workaround for the NPM dependency attacks. Certified Ethical Hacker, Certified Vulnerability Assessor (CVA), Certified AppSec Practitioner, Certified Network Security Specialist (CNSS), IBM Cyber Security Analyst.

Tanvinder Singh is a Director within the Cyber Security practice of PwC Malaysia. He has 18 + years of cross industry experience in defining, developing, and executing change and cybersecurity strategies in large organisations. He has a proven record of accomplishment as a thought-leader with broad subject matter knowledge in information security domains and success in developing and implementing cybersecurity technologies for large institutions. Tanvinder is adept at managing both projects and people, as seen through his experience in formulating technology strategy and platform architecture while leading momentous change initiatives across cybersecurity.

Dr. Syarifah Bahiyah Rahayu received the B.S.B.A. degree in Computer Information Systems from Northern Arizona University, USA, the M.Sc. degree in Information Technology from Queensland University of Technology (QUT), Australia, and the Ph.D. degree in Information Science from Universiti Kebangsaan Malaysia (UKM), Malaysia. She is currently the Director of the Cyber Security and Digital Industry Revolution Centre at the National Defence University of Malaysia (NDUM), where she also serves as a Senior Lecturer in the Faculty of Defence Science and Technology. Her academic and professional background spans both industry and academia. At NDUM, she has contributed to national digital defence initiatives and leads research on emerging technologies. Dr. Syarifah has published over 30 peer-reviewed articles in high-impact journals and international conference proceedings, and holds several intellectual property rights. Her research interests include cybersecurity, blockchain, artificial intelligence, image processing, and big data analytics. She is an active member of IEEE, the IEEE Education Society, and the IEEE Blockchain Community.

Registration Contract
Please complete this form immediately & email to tcharles@thomvell.com

RANSOMWARE RESILIENCE 2026

Preparing For the Next Generation of Cyber Attacks

19-20 January 2026 | Sheraton Imperial Hotel Kuala Lumpur

THOMVELL international Co. Reg. 679286-X

Confirm your seat with :

THOMVELL ☎ **+603 2260 6500**

Conference Fee (DDAS) 10% Discount

☐ Early bird : **USD 650.00 (Inclusive SST)**
Before 15 November 2025

☐ Training Fee : **USD 800.00 (Inclusive SST)**
After 15 November 2025

☐ Premier Plus**USD 1800.00 (Inclusive SST)**
For a group registration of
3 delegates from the same company

Details

Organization name:.....
Address:.....
Postcode:.....
Country:.....
Tel:.....
Fax:.....

Delegate

1. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
2. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
3. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
4. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
5. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....

Invoice

The Invoice should be directed to Mr / Ms / Dept:
Name:.....
Dept:.....
Tel:.....
Email:.....

Authorisation

Signatory must be authorized to sign on behalf of contracting organization

Name:.....
Job title:.....
Signature:.....
Email:.....
Telephone:.....
Mobile:.....

Venue

Sheraton Imperial Hotel Kuala Lumpur
Tel: 603-2717 9900

Hotel Accommodation:
Special rates have been negotiated with the hotel for conference delegates. Please make your bookings directly with Sheraton Imperial Hotel KL & indicate that you are attending.

Method of payment

Bank Transfer:

PAYMENT MUST BE RECEIVED BEFORE EVENT

Payment by bank transfer must indicate the invoice number

Account Name : **Thomvell International Sdn Bhd**
Bank Name : **Hong Leong Bank Bhd**
Account No. :**199 02000013**
Swift Code : **HLBBMYKL**

HRD CORP SBL KHAS CLAIMABLE
A 30% UPFRONT PAYMENT WILL BE REQUIRED PRIOR TO THE COMMENCEMENT OF THE CONFERENCE.

JomPAY **Biller Code:** 75788
Ref-1: Invoice Number

Cancellation

- Attendee substitutions are permitted up until two (2) business days prior to the conference. Please notify us in advance of any changes.
- Thomvell International does not provide refunds for cancellations. For cancellations received in writing more than seven (7) days prior to the event, you will receive a 100% credit for use at another Thomvell event within one year from the issuance date.
- Thomvell International assumes no liability in the event the conference is cancelled, rescheduled, or postponed due to fortuitous events, Acts of God, or unforeseen occurrences.
- Thomvell International reserves the right to cancel or modify the conference's content, timing, schedule or speakers, due to circumstances beyond its control.

3 EASY WAYS TO REGISTER

☎ **+603 2260 6500**
✉ 8-1, Jalan Tun Sambanthan 3, 50470 Kuala Lumpur
@ karen@thomvell.com / izzaty@thomvell.com

For official use only

Received: Date..... Code: **TVW4843**