The Institution of Engineers, Malaysia

HALF DAY SEMINAR ON

" WHY CORPORATE CYBERSECURITY IN MALAYSIA FAILS AND HOW TO IMPROVE IT DRASTICALLY – PART 1"

Organised by : Consulting Engineers, Special Interest Group, CESIG

4th April 2026, 9.00am - 1.00pm

METD Lecture Hall, 2nd Floor, Wisma IEM

Speaker

Ir. (Dr.) S. Vignaeswaran PEPC

BEM Approved CPD Hours : 4
Ref No. : IEM26/HQ/021/S

Why This Training Is Different

You will gain:

- Clear understanding of real cyber risk in Malaysia
- Practical frameworks you can apply immediately
- Simple language—no unnecessary technical jargon
- Malaysian laws, culture, and business environment
- Actionable strategies, not theory

Registration Fees (to include SST 8%)	
	RM
Student Member	100
Graduate Member	150
Corporate Member	250
Non Member	500

Time	Programme
8.30am	Registration Start
9.00am	Speakers Introduction by Chairman Ir. Tejinder Singh
9.05am	Why cybersecurity investments fail & Cybersecurity and Malaysian business culture
10.30am	Policy vs practice gaps & Human behavior and cyber risk
11.30am	Technology misuse and overdependence & Incident response failures
12.00pm	Building a sustainable cyber program & Measuring cyber success
12.45pm	Q & A Session
1.00pm	End of Seminar

Synopsis:

Cyberattacks in Malaysia are rising every year—targeting banks, hospitals, manufacturers, government agencies, SMEs, and universities. Yet many organizations still rely on outdated security thinking, fragmented tools, and checkbox compliance.

This training shows you why corporate cybersecurity fails in Malaysia—and exactly how to fix it.

The Reality in Malaysia Today

Malaysian organizations face:

- Increasing ransomware and data breaches
- Weak governance and unclear accountability
- Over-reliance on technology without strategy
- Low cybersecurity awareness at management level
- Compliance-driven security instead of risk-driven security
- Poor incident response readiness
- Skills gaps between policy and technical teams

Most failures are not technical—they are strategic, organizational, and human.

What This Training Will Teach You

This program explains cybersecurity from the business, governance, and technical perspectives—using Malaysian context, regulations, and real-world cases.

You will learn:

✓ Why cybersecurity programs fail despite heavy spending
✓ How board and management decisions create hidden cyber risks
✓ How to align cybersecurity with business strategy
✓ How to move from compliance-based to risk-based security
✓ How to build practical cyber governance structures

Who Should Attend

This training is designed for:

• CEOs, Directors, and Board Members
• CIOs, CISOs, IT Managers
• Risk, Compliance, and Audit Professionals
• Business Unit Heads
• Government and GLC Officers
• Cybersecurity Practitioners
• University and Training Institution Leaders

No heavy technical background required—business and IT professionals will benefit equally.

Speakers Biodata

Ir. (Dr.) S. Vignaeswaran PEPC has more than 40 years of working experience in the electrical, computer, IT, SCADA, project management and tendering field. He has been involved in state-of-the-art applications which includes operational technology (OT) cyber-security from the 1990s. He has an Electrical Engineering degree from Monash University (Clayton, Australia), MSc in IT/BIS from University of Keele, UK and a PhD in CyberSecurity from Alabama, USA. He continues to publish cutting-edge research papers in the Engineering, IT, Computer Security and Project Management fields and is now writing a book on Corporate Cybersecurity. These have been based on his role as the Client's HoD (Electrical & Automation) in a RM 8 billion Saudi Arabian project. All of these three international degrees and his specialized experiences, has allowed the speaker to conduct PhD supervision in Malaysia to the highest standards, requirements and compliances. His venture into the Smart City market segment consolidates his expertise in the Electrical, Automation, Project Management etc, among others. It is his ambition to bring Smart Cities into reality while opening up new market segments for Information Technology (IT) and Operational Technology (OT) specialists. He is currently involved in the research of a state-of-art utility automation, IT and engineering systems that applies Cybersecurity, AI and pre-emptive decision-making models with innovative solution approaches. He has set up MALAYSIA SMART INTELIGENT TECHNOLOGICALLY INTEGRATED CITY (MySITI) special interest group under the MALAYSIAN SOCIETY FOR ENGINEERING AND TECHNOLOGY (MySET) to realize his hopes and achieving his objectives, both locally and internationally.

Why This Training Is Different
Most cybersecurity courses focus on tools. This course focuses on why tools fail

You will gain:
• Clear understanding of real cyber risk in Malaysia
• Practical frameworks you can apply immediately
• Simple language—no unnecessary technical jargon
• Malaysian laws, culture, and business environment
• Actionable strategies, not theory

What You Will Be Able to Do After This Training
After completing this program, you will be able to:

✓ Identify root causes of cyber failure in your organization
✓ Challenge ineffective cybersecurity spending
✓ Design a realistic cybersecurity roadmap
✓ Improve leadership involvement in cyber risk
✓ Strengthen policies, people, and processes
✓ Communicate cyber risk clearly to management and board
✓ Reduce incidents, losses, and downtime

Key Topics Covered
• Why cybersecurity investments fail
• Cybersecurity and Malaysian business culture
• Leadership and governance failures
• Policy vs practice gaps
• Human behavior and cyber risk
• Technology misuse and overdependence
• Incident response failures
• Building a sustainable cyber program
• Measuring cyber success

The Value to You and Your Organization
This training helps you:
• Protect reputation and customer trust
• Reduce financial and operational losses
• Improve regulatory confidence
• Strengthen business resilience
• Make smarter cybersecurity investments
• Lead cybersecurity—not just manage it

Take Control of Cyber Risk
Cybersecurity failure is not inevitable. With the right mindset, structure, and leadership—it can be drastically improved. Join this professional training and learn how to turn cybersecurity from a weak point into a strategic advantage. Because in today's Malaysia, cybersecurity is no longer an IT issue — it is a business survival issue.