



**YAMADA  
CONSULTING  
& SPIRE**

# **Securing the Edge:** Cyber Threats, Customer Shifts & Investment Signals in Southeast Asia

YAMADA CONSULTING & SPIRE



# Agenda

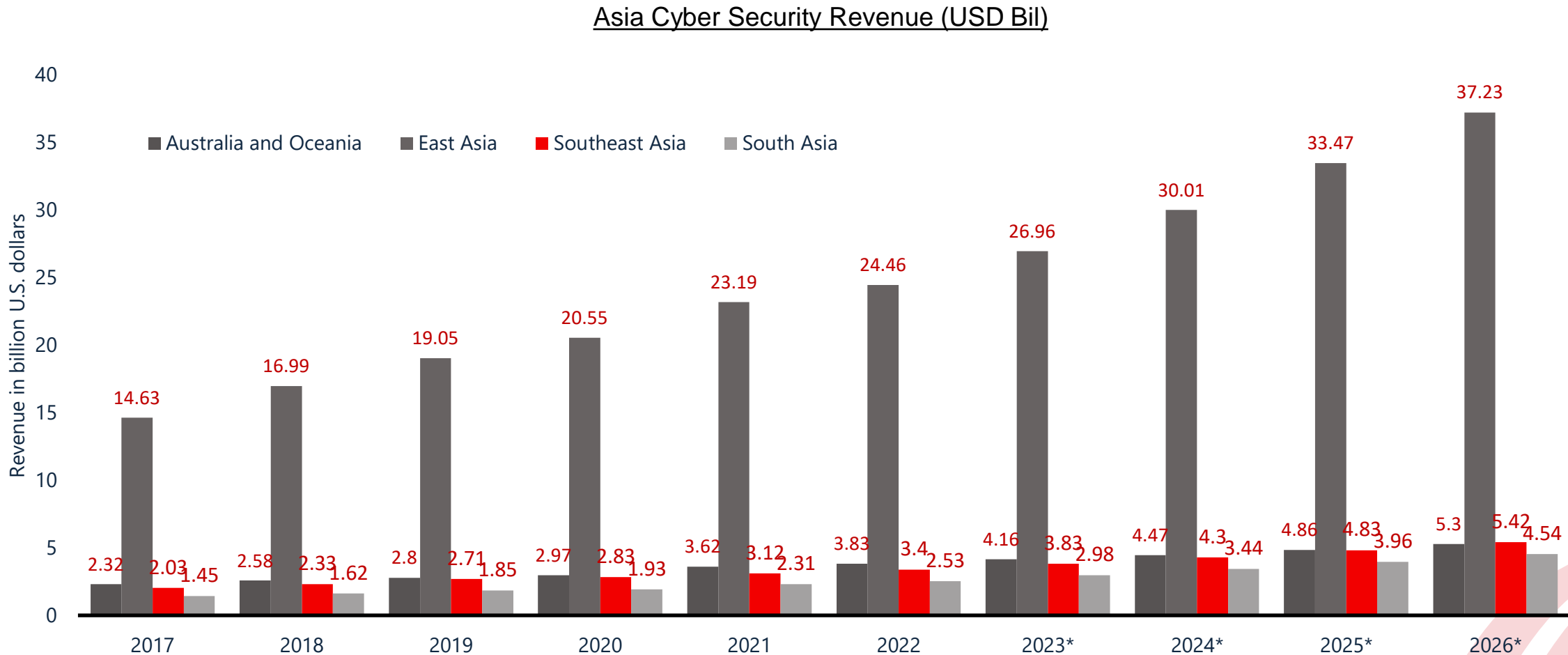
- **S.E Asia Cybersecurity Market overview**
- **S.E Asia under threat**
- **How are IT managers responding (Emerging market needs)**
- **Cybersecurity sector as an investment opportunity**

## ○ S.E Asia Cybersecurity Market overview

- S.E Asia under threat
- How are IT managers responding (Emerging market needs)
- Cybersecurity sector as an investment opportunity

# S.E Asia Cybersecurity Market overview

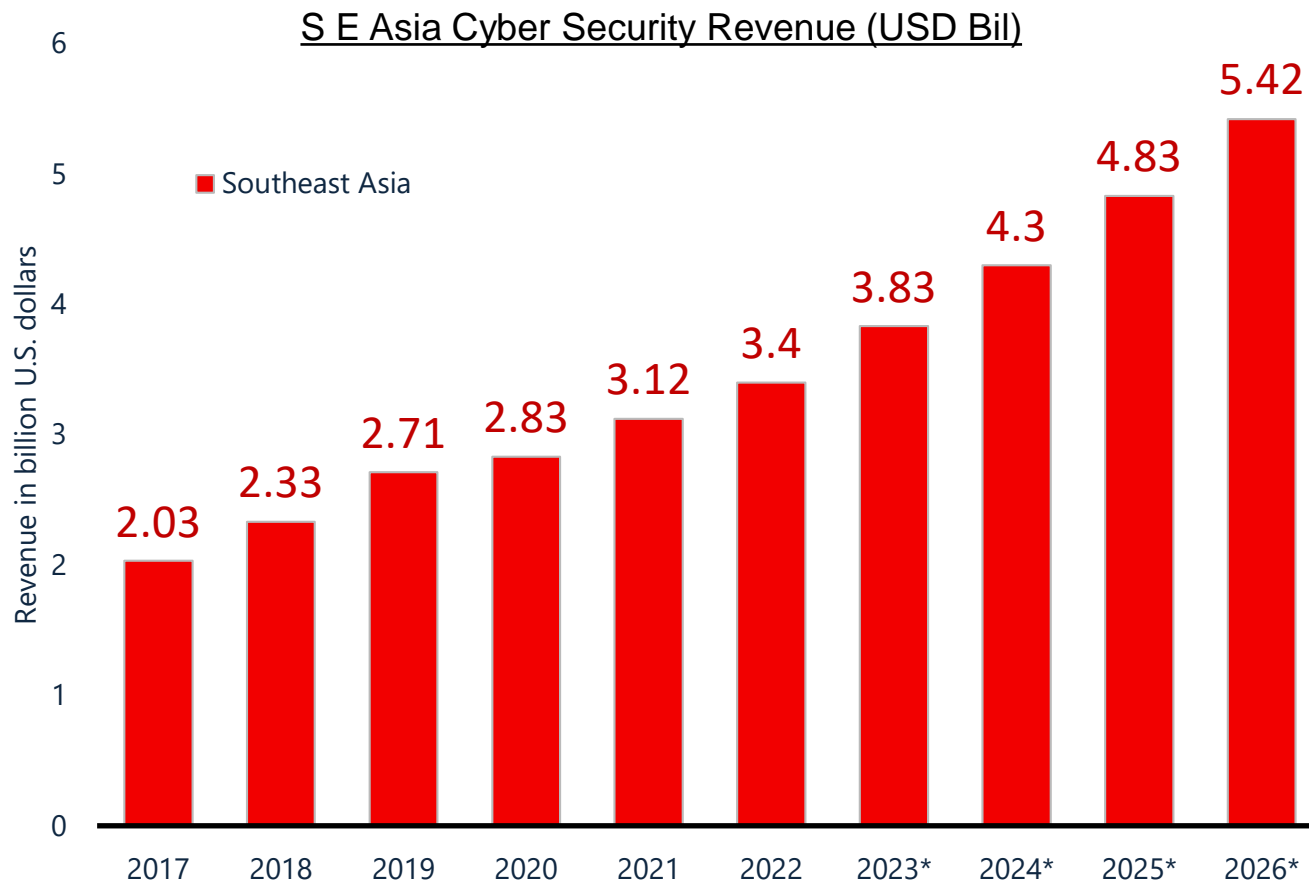
The S.E Asia market comprises 10% of USD 40 Bil market in Asia dwarfed by larger markets in China, Japan and Korea



Source: Statista

# S.E Asia Cybersecurity Market overview

Never the less, SE Asia cybersecurity expenditure is still USD 3-4 Bil market growing steadily at 11-12%

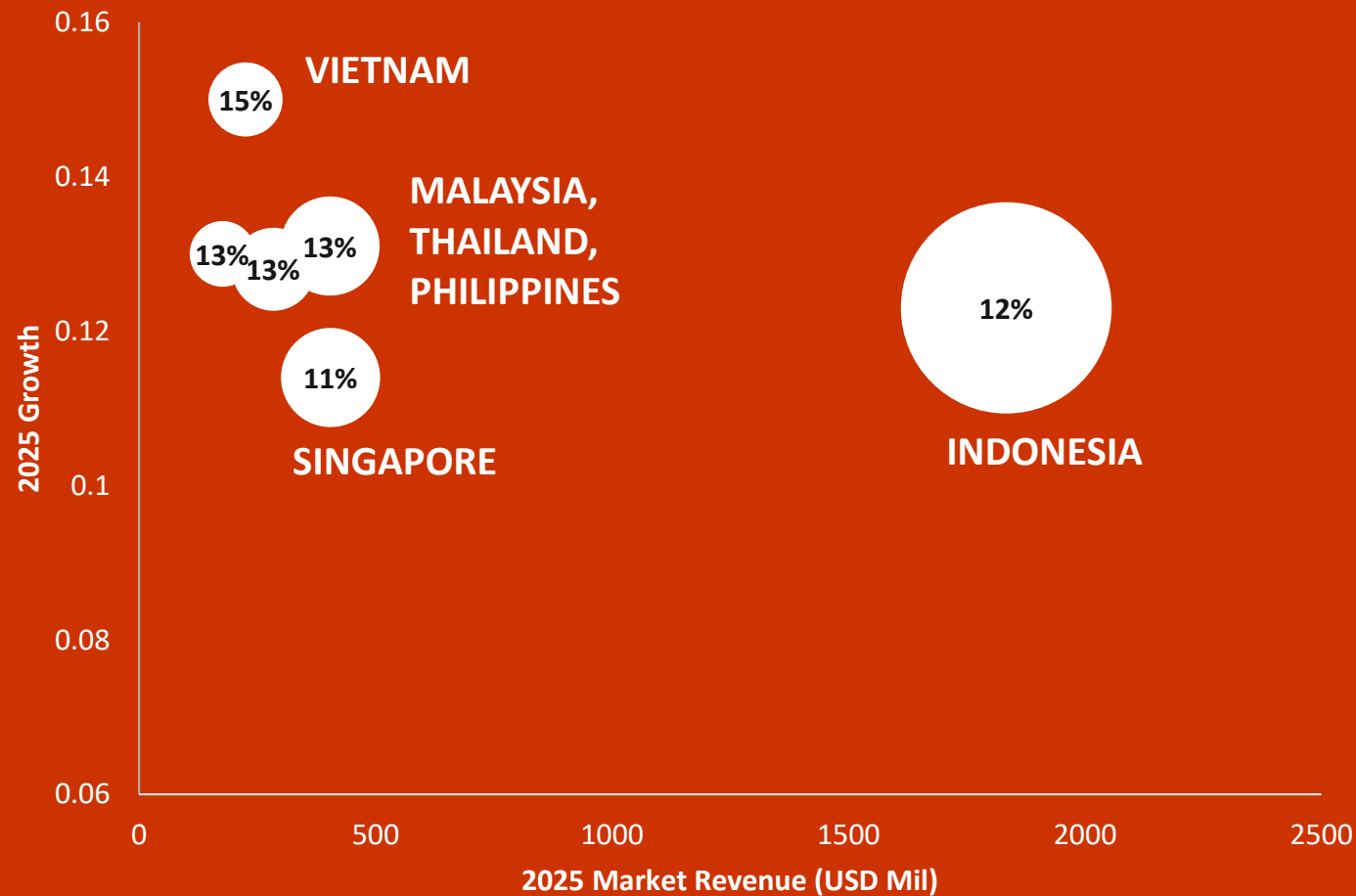


- Digital transformation amongst companies
- Rising cyber threats
- Government Initiatives (cyber security and PDPA drive in Singapore, Indonesia, Malaysia etc.)
- Growth of fintech and cryptocurrencies
- Vibrant investment and start-up environment

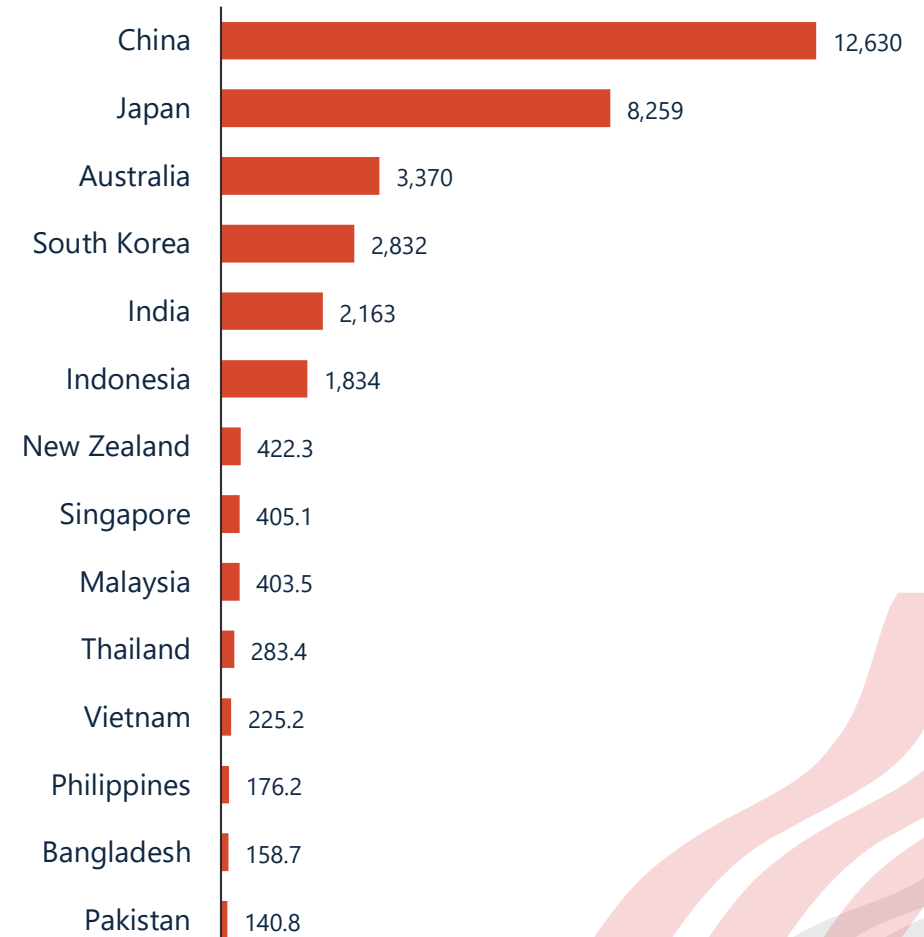
# S.E Asia Cybersecurity Market overview

Individual Countries vary in size and growth prospects. Indonesia is larger and more mature, while Vietnam shows growth potential

## Asia 2025 Size and Growth



## Cyber Security Revenue in USD Mil



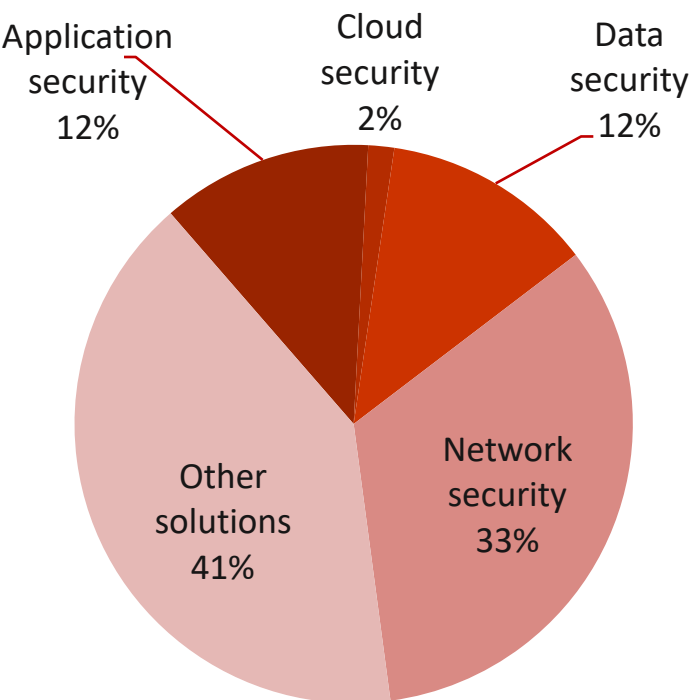
Source: Statista

# S.E Asia Cybersecurity Market overview

Still early Days...

Network Security and local data security dominate the solutions offered

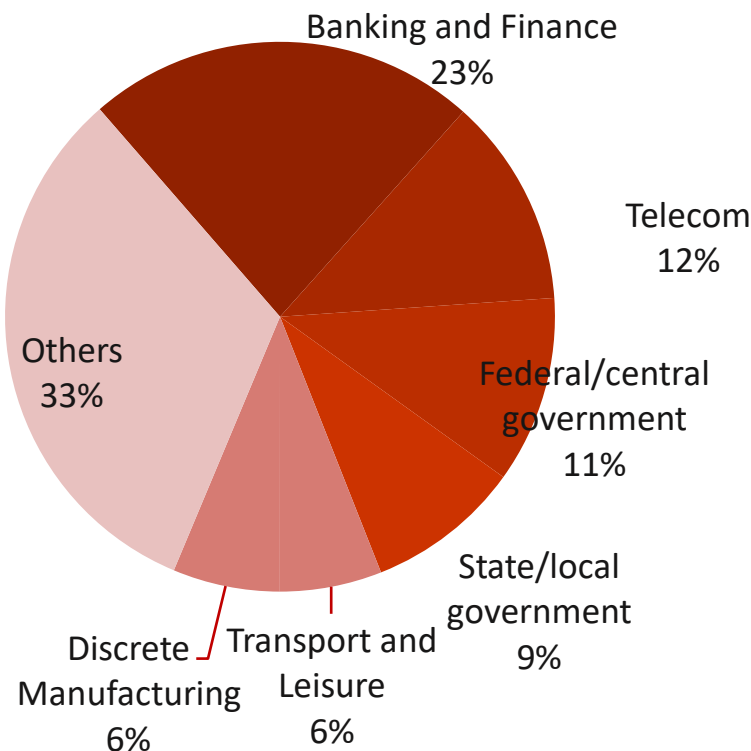
2024 Cyber Security spend by solution



Source: Statista

The Market is still nascent as most serious demand is still from a selected set of critical sectors

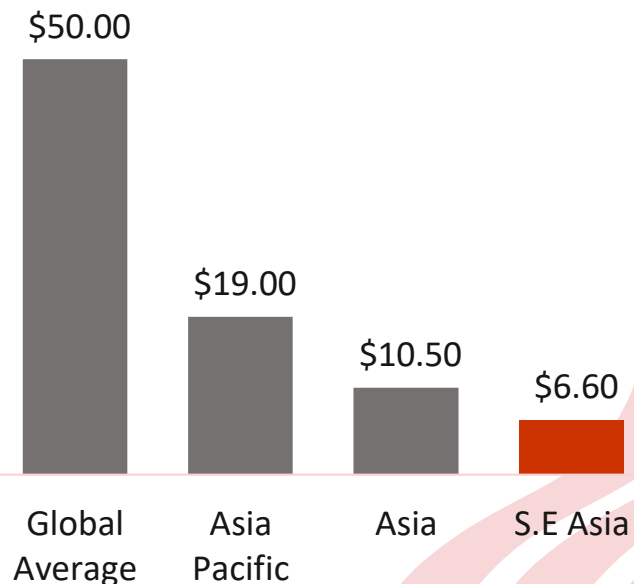
2024 Cyber Security spend by sector



Source: IDC

There is room for more sophistication, as spend per employee vastly lags behind other regions

2024 Cyber Security spend per Employee (SE Asia vs other Regions)



Source: PwC ASEAN Digital Trust Insights 2023, Y&S Estimates



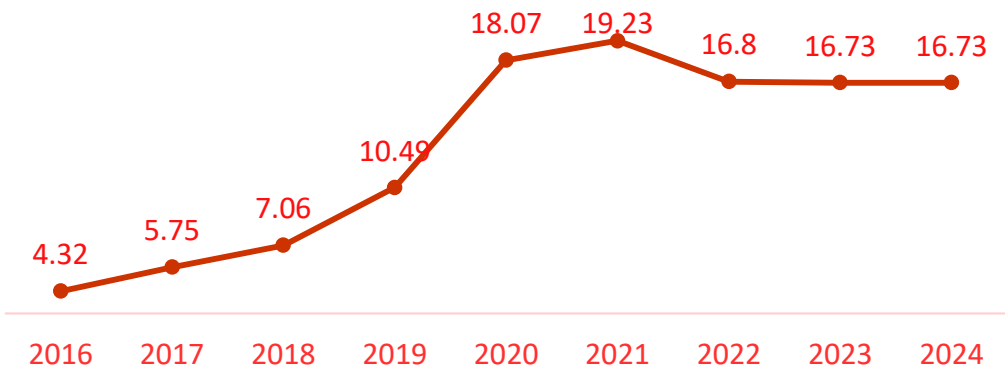
- S.E Asia Cybersecurity Market overview
- **S.E Asia under threat**
- How are IT managers responding (Emerging market needs)
- Cybersecurity sector as an investment opportunity



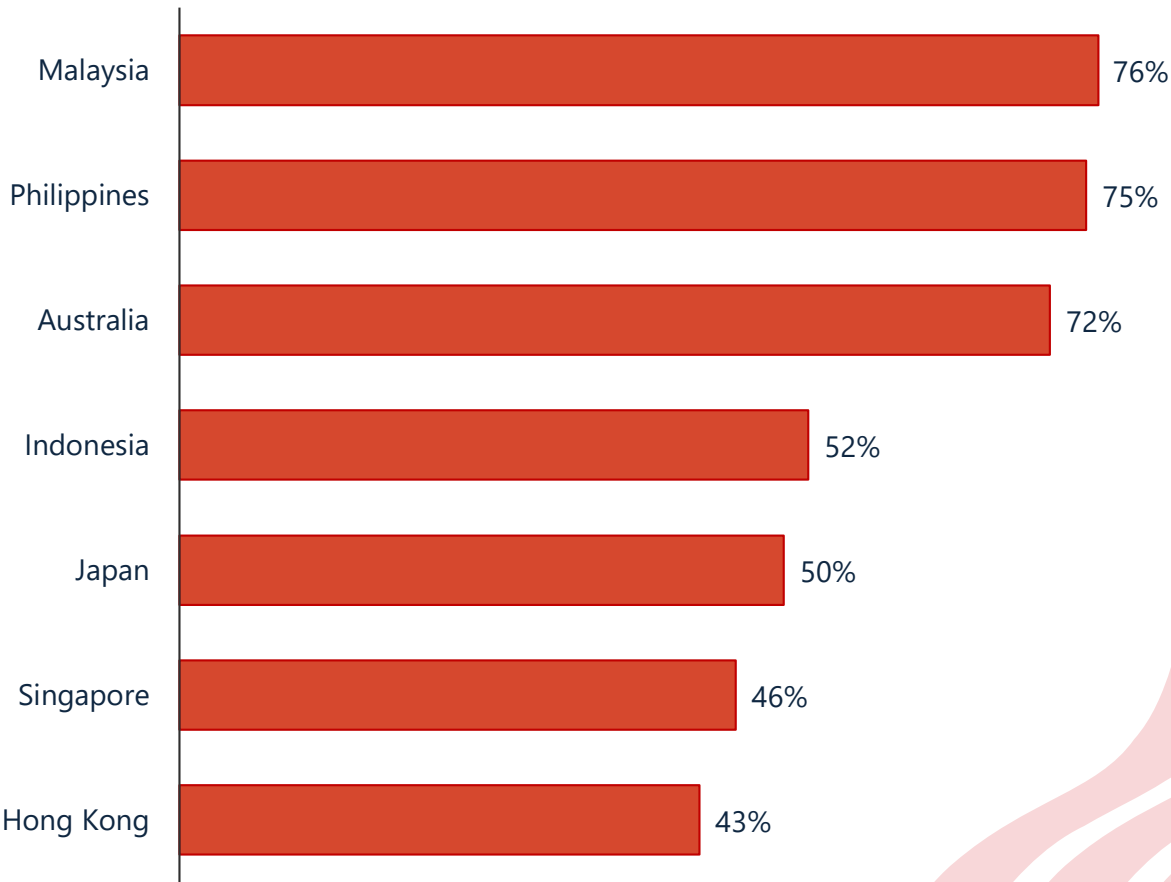
# S.E Asia Under Threat

Cyber attacks globally are stabilizing but the threat landscape has changed in the last 4 years with Asia Pacific Accounting for 34% of the cyber attacks globally

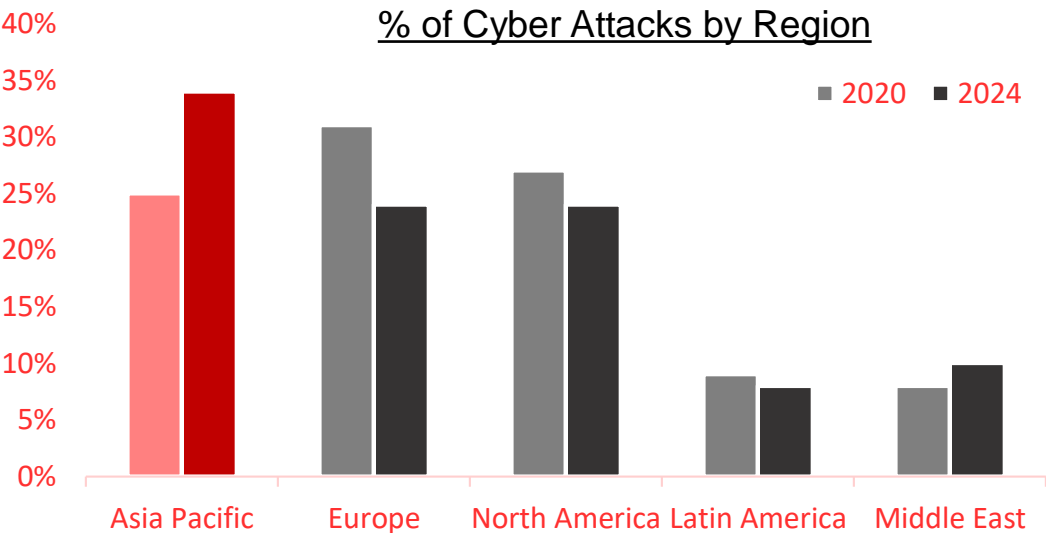
Volume of Cyberattacks Globally (in Mil)



% of Companies that have Experience Cyber Incidents



% of Cyber Attacks by Region



Source: Statista, IMF

Source: Kroll

# S.E Asia Under Threat

National Cyber Security Index (Measure of Preparedness) varies across the region. Singapore and Malaysia are most developed, but others need tighter infrastructure

## STRATEGIC METICS

- Policy Development
- Global Contribution
- Educational /Professional Development
- Domestic R&D

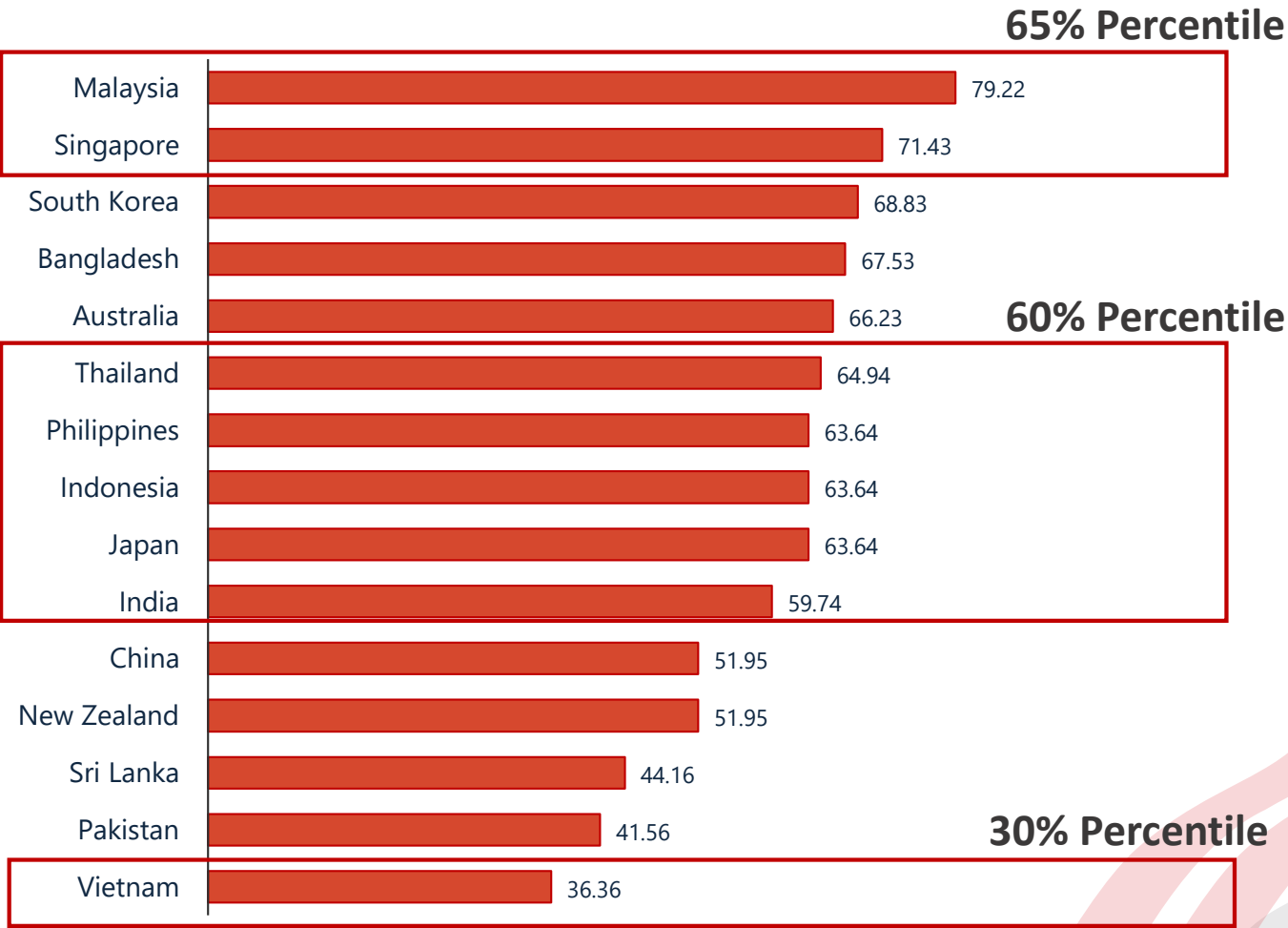
## PREVENTIVE METRICS

- Essential Services
- Digital Enables
- Threat analysis and Awareness
- Personal Data Protection

## RESPONSIVE METRICS

- Cyber Incident Response
- Cyber crisis Management
- Fight against cybercrime
- Military cyber defense

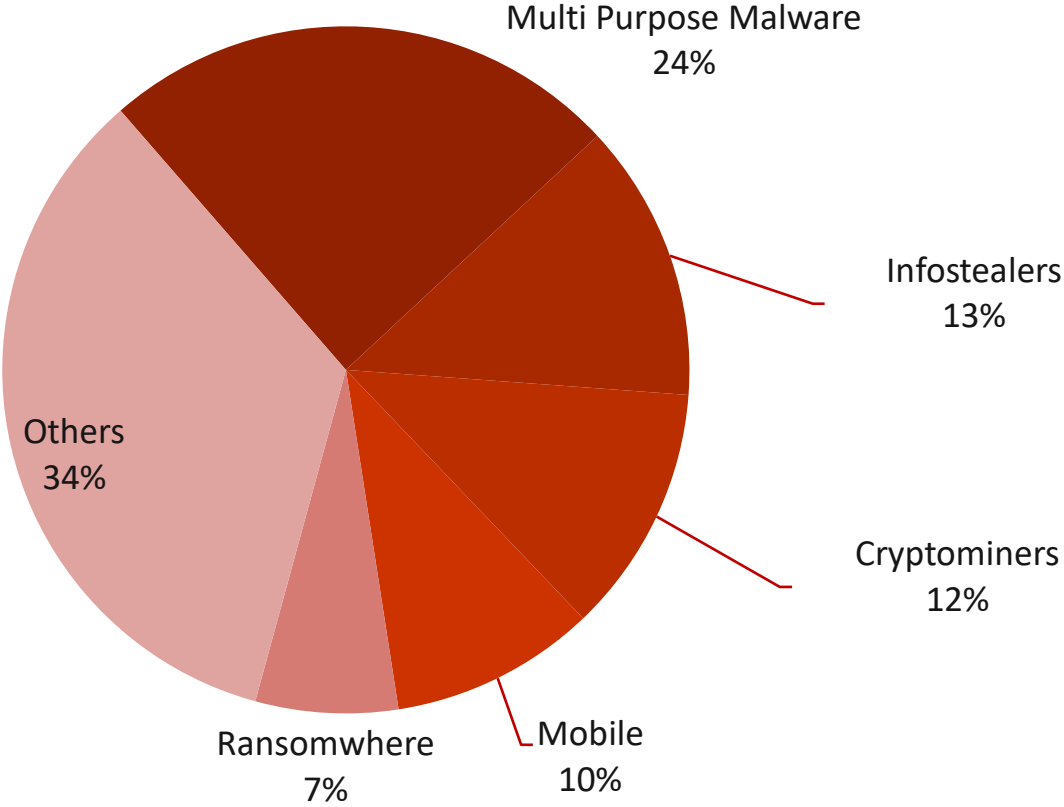
Source: NCSI



# S.E Asia Under Threat

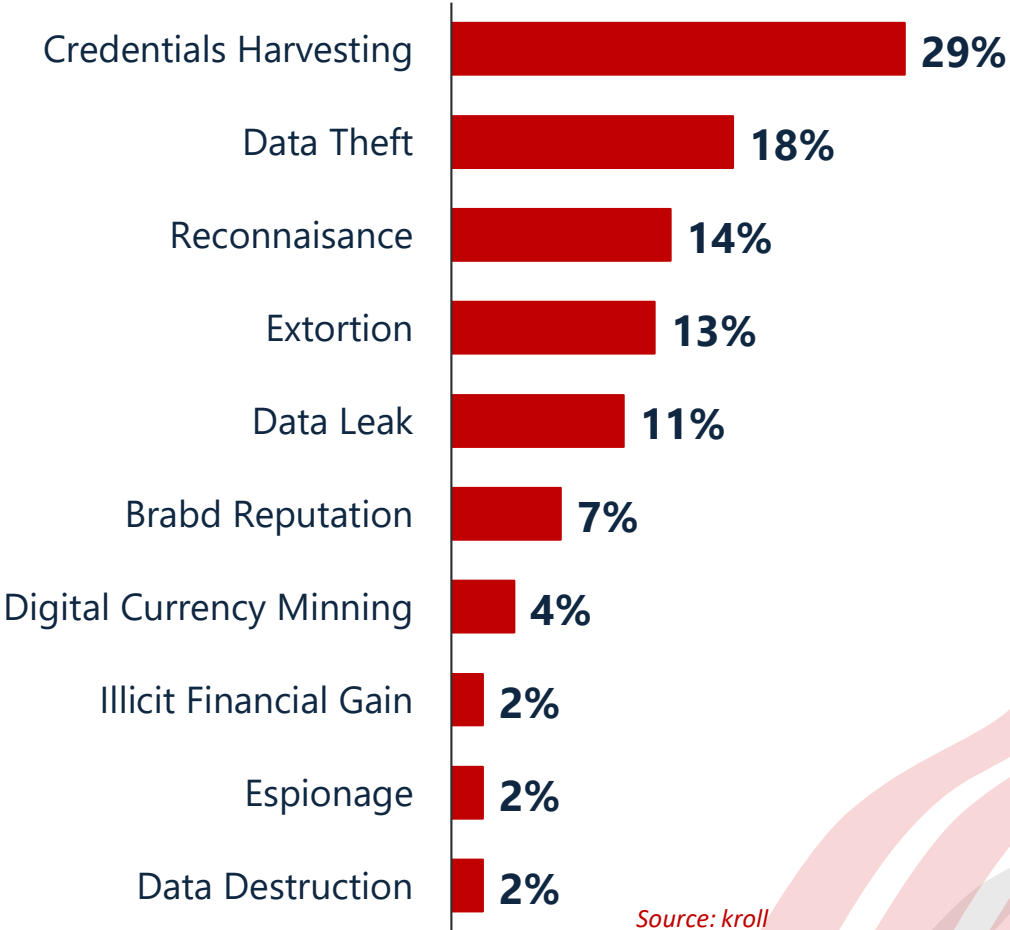
Type of Attacks and their Impact- Theft of credentials and Data have been most prevalent

Type of Cyber Attacks 2024



Source: Cyber Security Report 2024- Checkpoint software technologies

Top impacts observed in incident response 2024 (IBM Cyber Security Report)



Source: kroll

# S.E Asia Under Threat

The Enemy is evolving with automated reconnaissance lower entry barriers & AI



**Cloud attacks are evolving but misconfigurations still lead:**

Cloud environments are the top targets, where adversaries exploit misconfigurations, compromised identities, and insecure APIs.



**AI is taking cybercrime to the next level:**

Bad elements are using AI for phishing, impersonation extortion and evasion tactics. Deepfakes, phishing websites and synthetic voices are taking the scale of cyberthreats to unprecedented levels



**Reconnaissance is Surging:**

Cybercriminals are deploying Automates scanning tools to identify soft targets. 2024 scans amounted to 36000 scans per second globally



**Exploitation Volumes are rising, but time to exploit is steady:**

Time between disclosed vulnerability and exploitation is steady at 5.4 days. However the volume of exploitation incidents reached 97Billion in 2023.



**CaaS (Cybercrime as a service) has made crime easier:**

CaaS has lowered barriers to entry for smaller criminals. The volume of stolen credentials and direct corporate access has risen by 500%



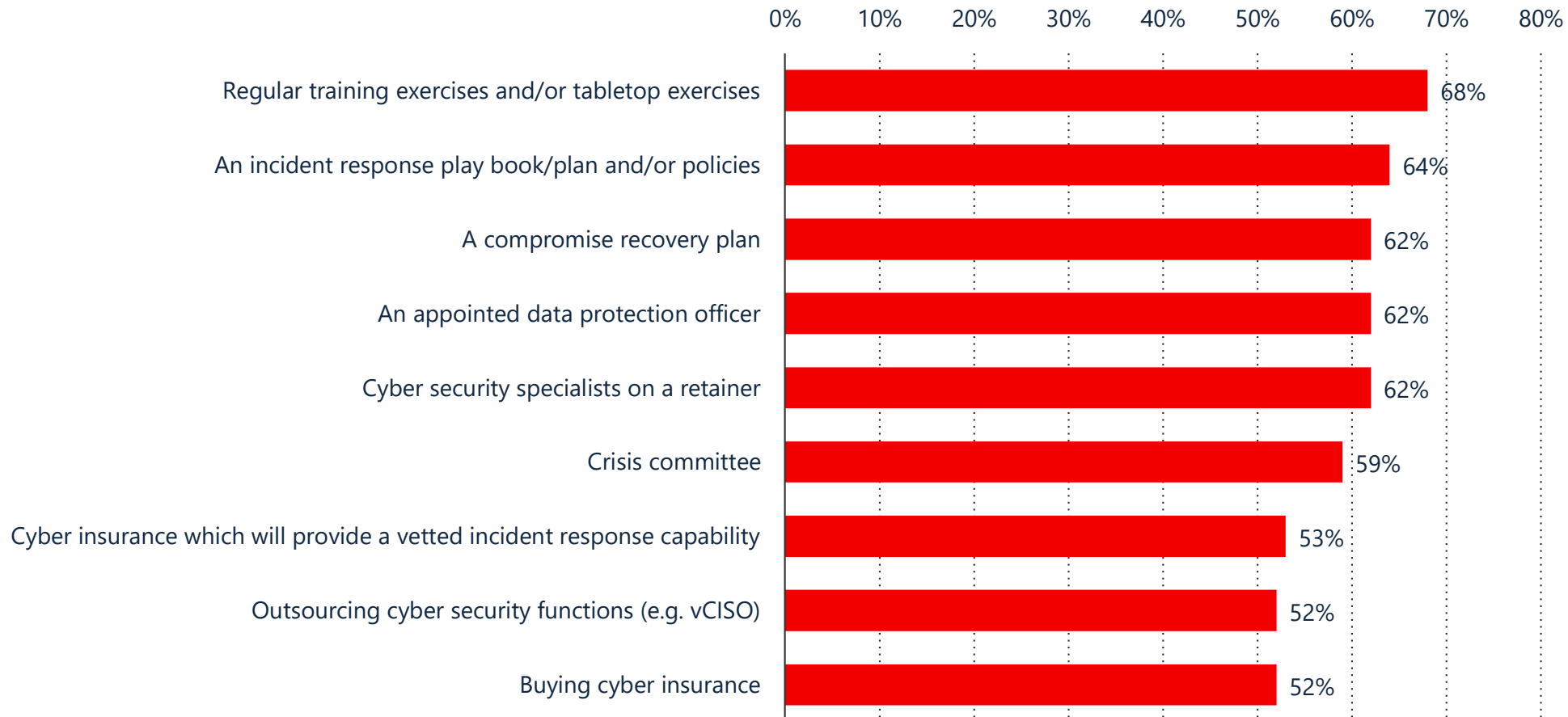
**Post Exploitation tactics are getting stealthier:**

Criminals use a host of tactics like Active Directory Manipulation, RDP based lateral movement and encrypted C2 via DNS and SSL to cover their tracks

- S.E Asia Cybersecurity Market overview
- S.E Asia under threat
- How are IT managers responding (Emerging market needs)
- Cybersecurity sector as an investment opportunity

# How IT are managers responding (Emerging market needs)

By 2022 Concrete steps had been taken by over 50% of the enterprises



# How IT are managers responding (Emerging market needs)

Further Progress has been made in improving security and mitigating Risks in the last 4 years

## Claimed Achievements from 2020-2024



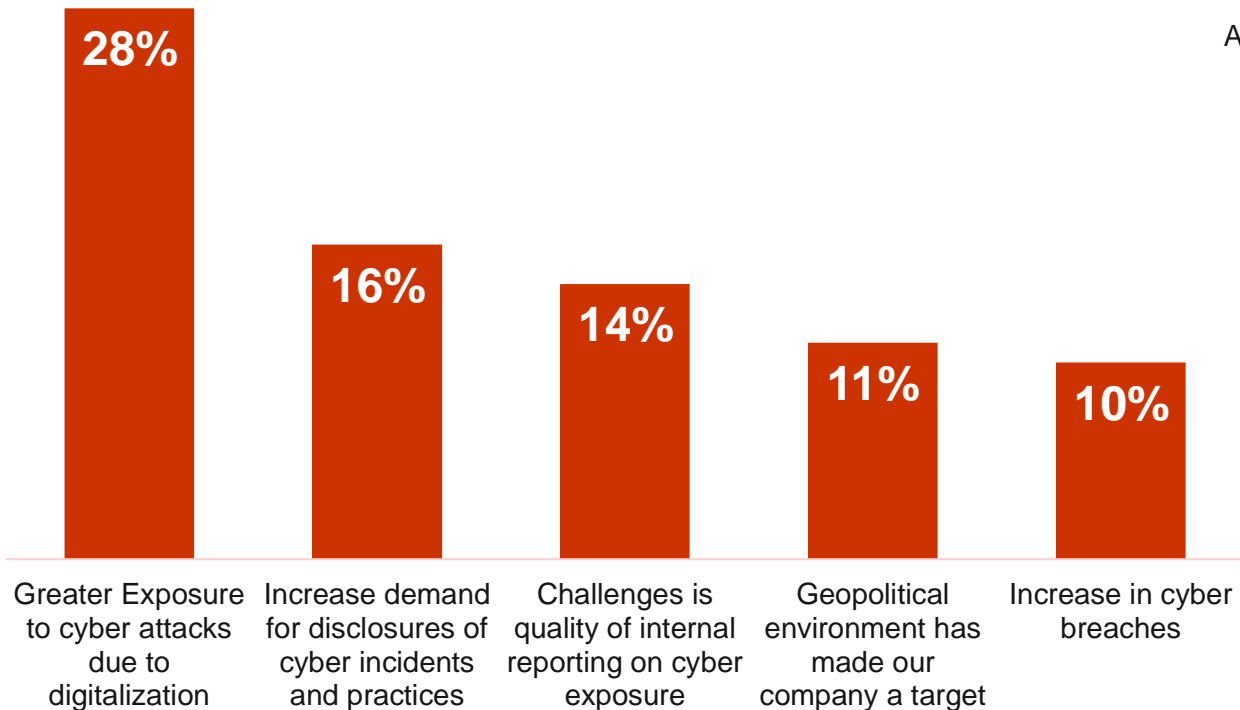
Source: Digital Trust Insights 2024: Asia Pacific | PwC



# How IT are managers responding (Emerging market needs)

## But Cyber security continues to be a gap, as IT managers see an impending need

S.E Asian Enterprises say they experienced the following in the last 3 years...



Source: Digital Trust Insights 2024: Asia Pacific | PwC

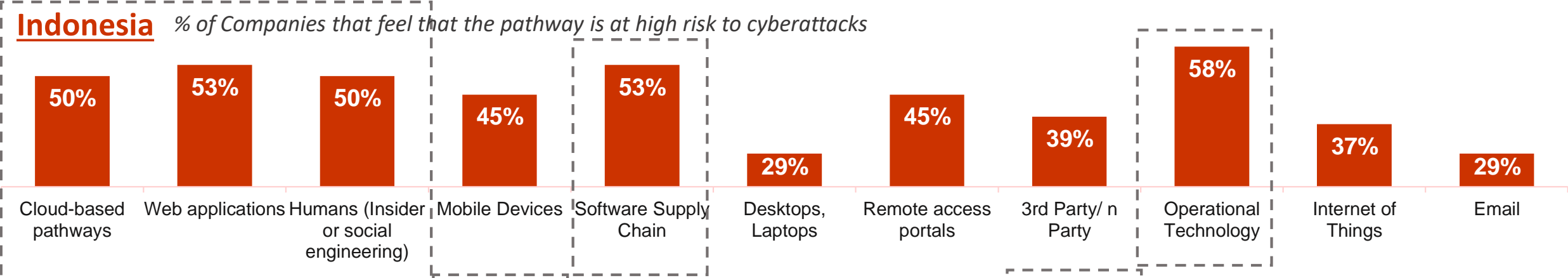
S.E Asian Enterprises expect the following threats to increase...



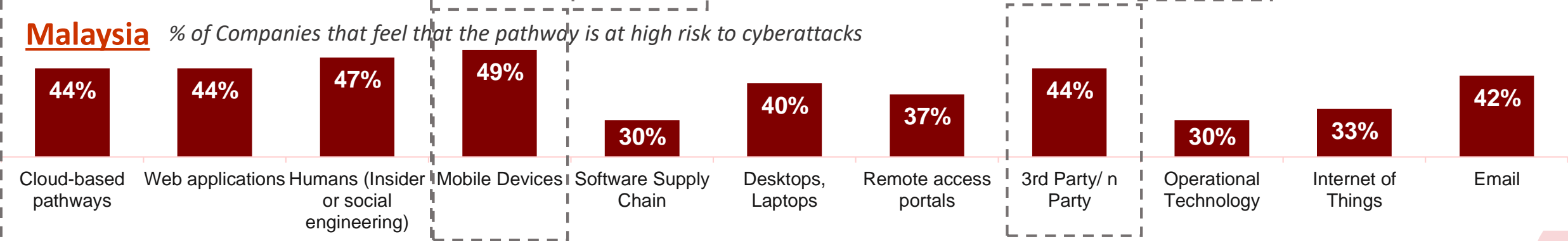
# How IT are managers responding (Emerging market needs)

Cloud, email and Web-related pathways are most at-risk to adversaries' attack

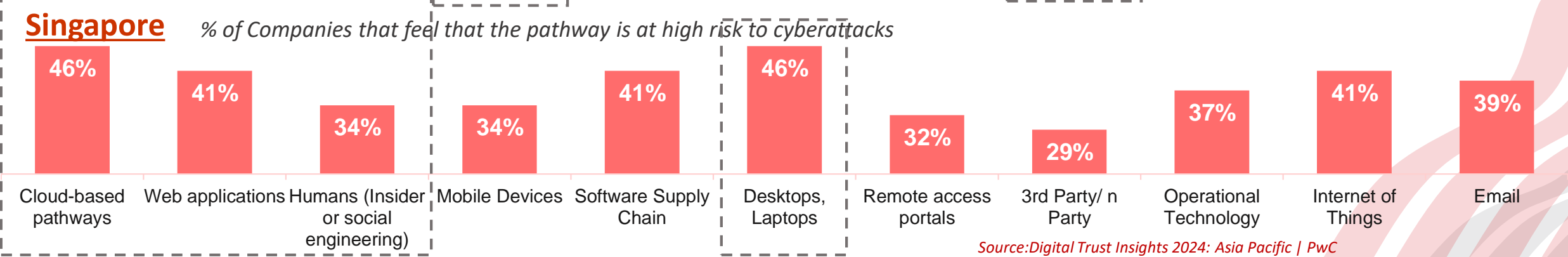
**Indonesia** % of Companies that feel that the pathway is at high risk to cyberattacks



**Malaysia** % of Companies that feel that the pathway is at high risk to cyberattacks



**Singapore** % of Companies that feel that the pathway is at high risk to cyberattacks

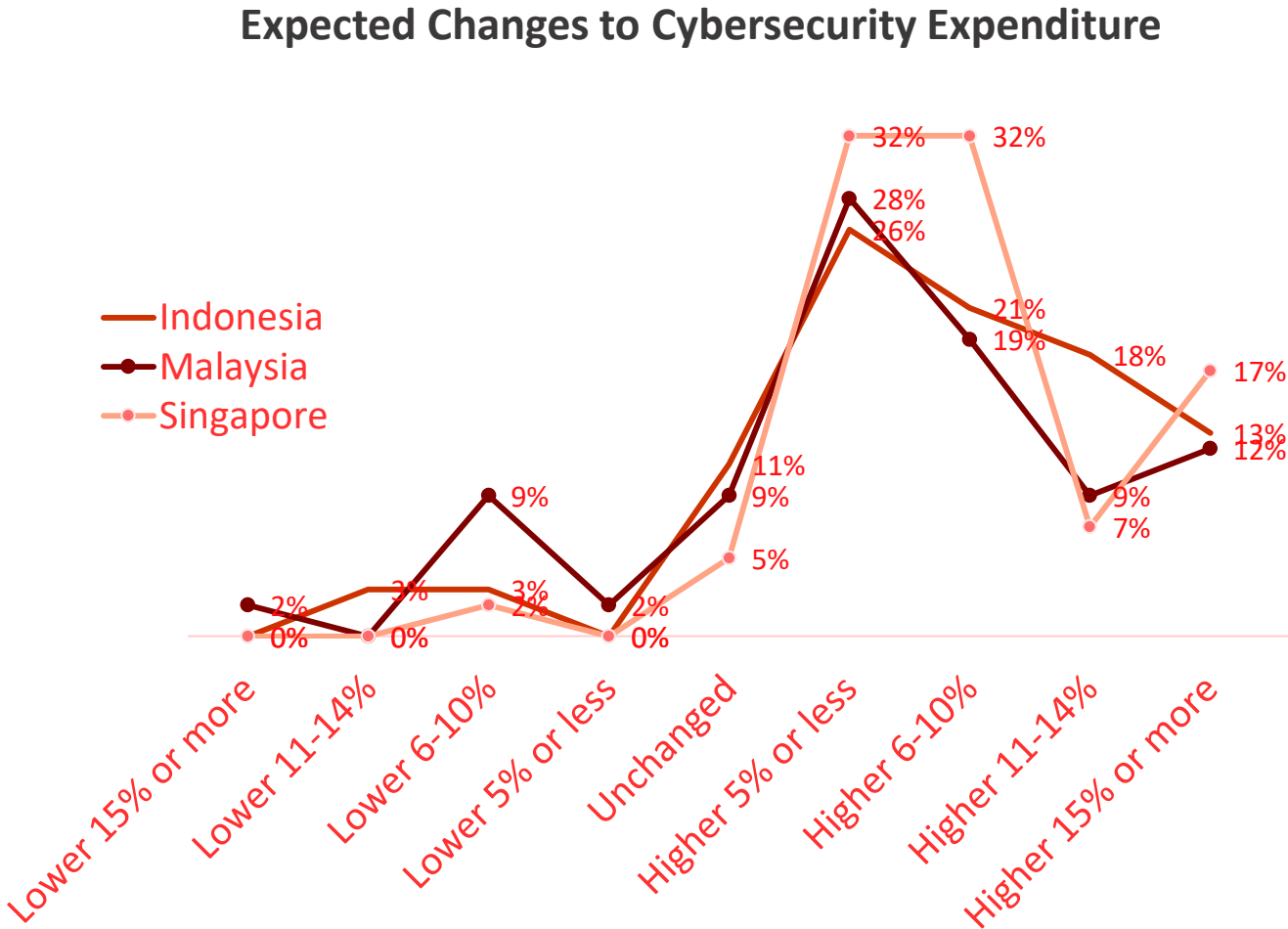


Source: Digital Trust Insights 2024: Asia Pacific | PwC

# How IT are managers responding (Emerging market needs)

Enterprises are expected to increase spending on cybersecurity by 5-10%

**11-13%**  
of IT Budgets are allocated to Cyber security



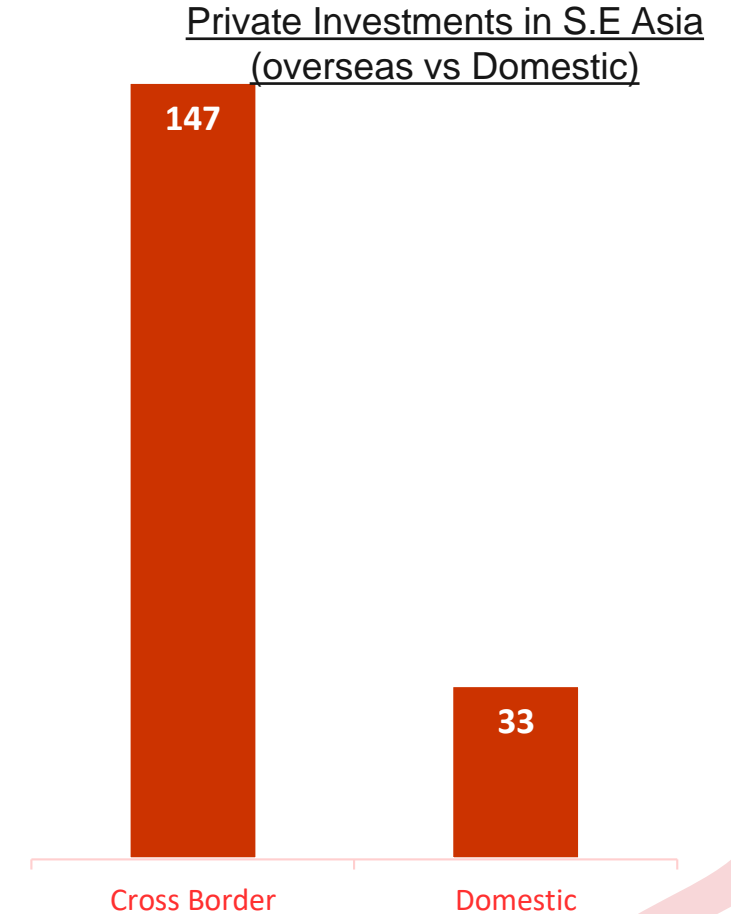
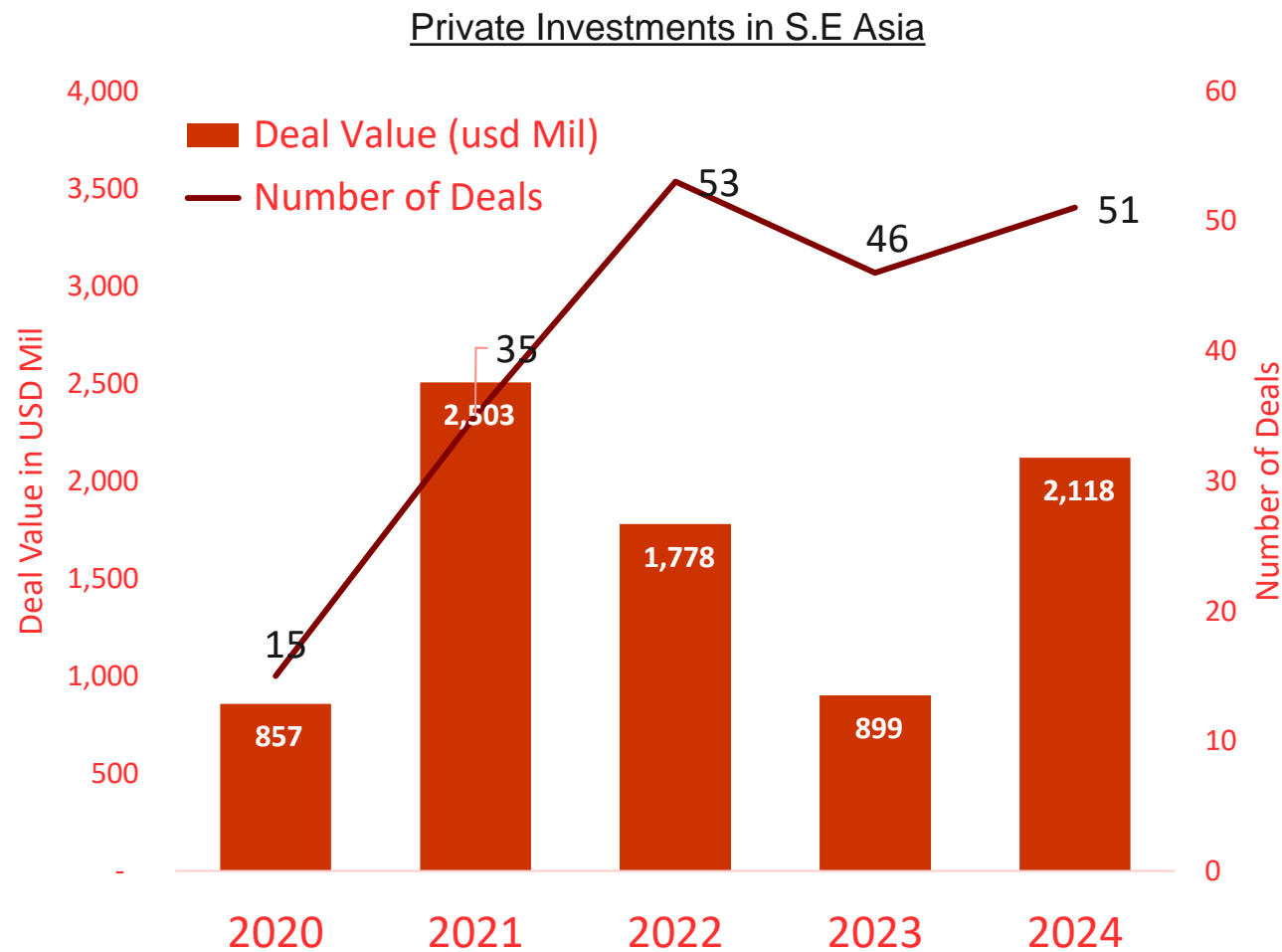
**60%**  
Of successful cyberattacks in 2023 lead to damages

**>\$ 100,000**

- **S.E Asia Cybersecurity Market overview**
- **S.E Asia under threat**
- **How are IT managers responding (Emerging market needs)**
- **Cybersecurity sector as an investment opportunity**

# Cybersecurity sector as an investment opportunity

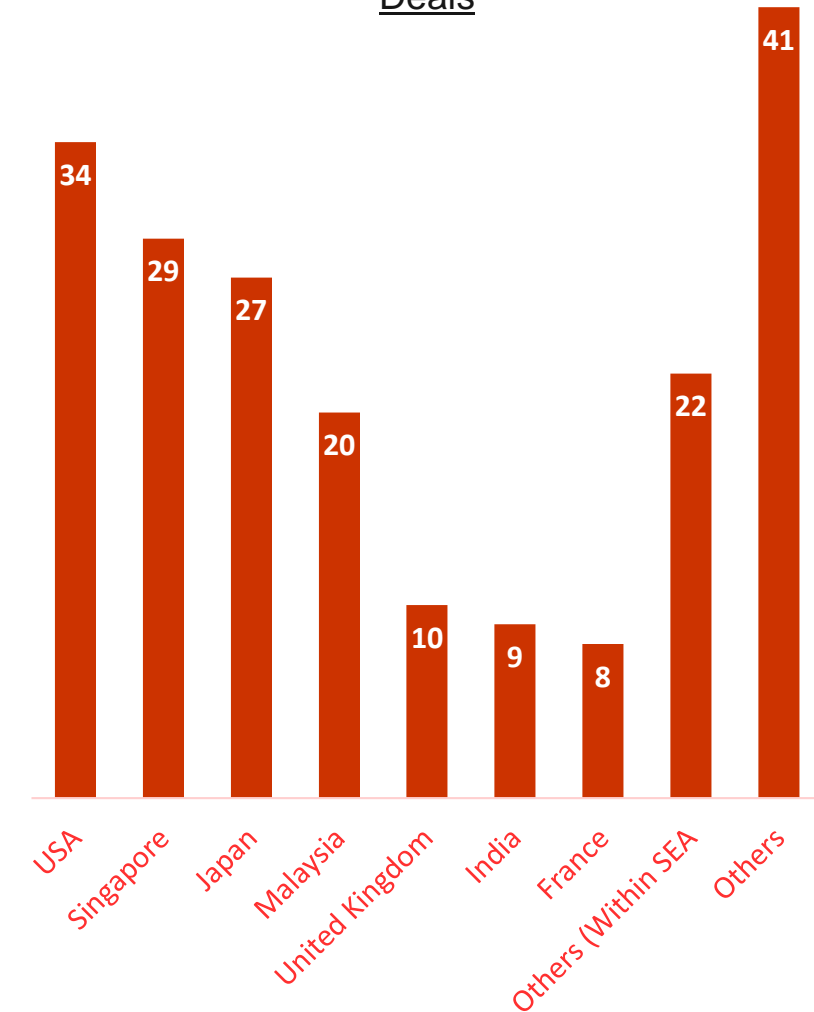
Over USD 8 Bn of private investments and 180 M&A deals have taken in place in the sector in the last 5 years



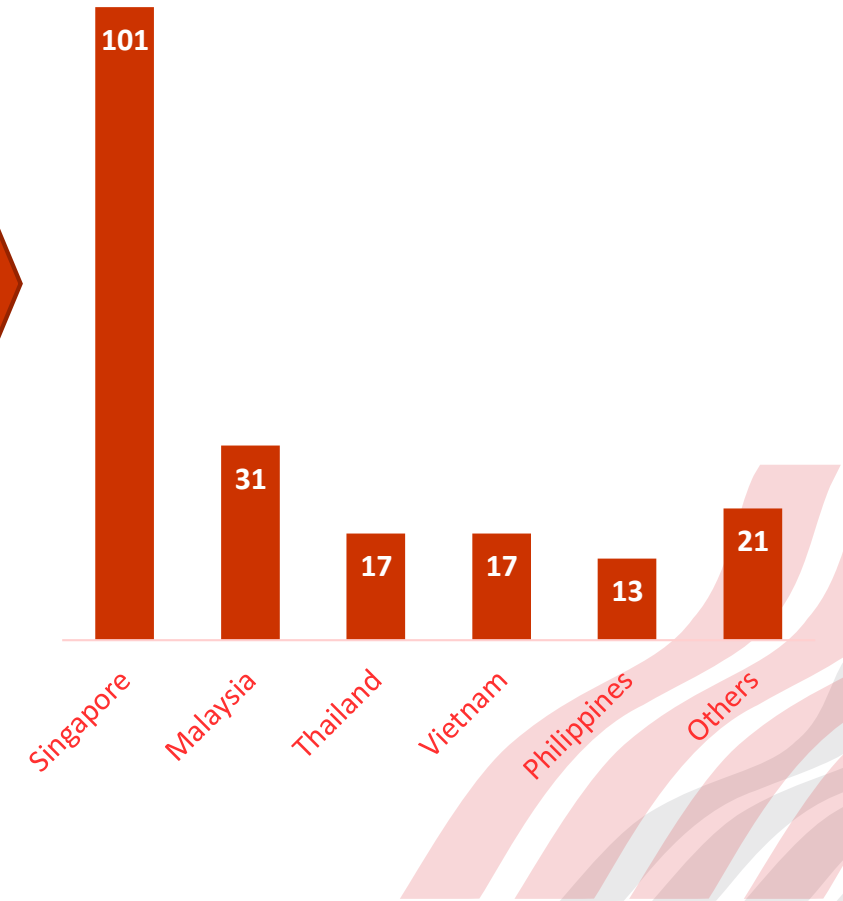
# Cybersecurity sector as an investment opportunity

Majority of the deals have been from overseas and into Singapore

Source of Overseas Investment Deals



Destination of Overseas Investment Deals



Source: Y&S Analysis, Mergers & Markets

Strictly Private & Confidential 2025

# Cybersecurity sector as an investment opportunity

## Notable Deals

2025	2025	2024	2023	2022
GMO Internet Inc (Japan)	BitDifender Srl (Romania)	TechMatrix Corp (Japan)	Armor Defense Inc (USA)	SK Inc (South Korea)
\$14 Mn	Undisclosed	\$1.1Bn	Undisclosed	\$1.0Bn
NetDesign Holdings (Thailand)	Bitshield Data Defense (Malaysia)	Firmus Sdn Bhd (Malaysia)	Quantum Security (Singapore)	TES Pte Ltd (Singapore)
<p>Japanese tech conglomerate GMO Internet Inc strategically bolstered its regional presence in Southeast Asia by acquiring 49% stake in a multi-national connectivity and security player.</p> <p>The target has presence in Thailand, Philippines, Vietnam, Laos</p>	<p>BitDefender, one of Europe’s leading endpoint protection vendors, fully acquired Malaysia-based Bitshield. This move suggests BitDefender’s intent to use Malaysia as a launchpad into Southeast Asia, leveraging local presence for APAC market penetration.</p>	<p>The largest cybersecurity deal in Malaysia, signaling Japan’s sustained interest in regional cyber capabilities. TechMatrix likely aims to integrate Firmus’ consulting and managed security services into its broader digital solutions business.</p>	<p>Armor Defense’s acquisition of Quantum Security (Cybersecurity Software) is a classic “buy &amp; build” strategy. Singapore’s regulatory and tech-friendly environment made it a preferred regional hub. This deal likely provides operational and market access advantages.</p>	<p>Private SK Inc’s acquisition of TES reflects its ambition to strengthen end-to-end IT lifecycle management and cybersecurity capabilities. TES’s global e-waste and ITAD (IT Asset Disposal) services provide compliance-critical cybersecurity assurance to enterprises.</p>

Source:Y&S Analysis, Mergers & Markets



# Cybersecurity sector as an investment opportunity

## M&A Strategic Investor Checklist

<b>1. Market Opportunity</b> Size, urgency, and growth potential	<ul style="list-style-type: none"> <li>- Addresses fast-growing verticals (e.g. Gov, Fin)</li> <li>- Operating in fast growing market (eg Malaysia, Indonesia, Philippines etc.)</li> <li>- Strong pipeline in at least 2-3 SEA markets</li> </ul>	<b>5.Customer Base &amp; Stickiness</b> Quality and retention of clients	<ul style="list-style-type: none"> <li>- 10+ paying enterprise customers in SEA</li> <li>- High cross-sell/up-sell ability</li> <li>- Multi-year SaaS or MSSP recurring revenue model</li> <li>- Low churn, stable gross margins</li> <li>- Flexible pricing tiers for SMEs</li> </ul>
<b>2. Product-Market Fit</b> Relevance and stickiness of the product	<ul style="list-style-type: none"> <li>- Proven demand from local clients</li> <li>- High renewal rates or early ARR traction</li> <li>- Tailored for SEA use cases (e.g., cloud security, SME digitalization)</li> </ul>	<b>6. Talent &amp; Execution Team</b> Strength and relevance of the execution team.	<ul style="list-style-type: none"> <li>- Deep cyber expertise and/or prior start-up exits</li> <li>- Regional experience and execution track record</li> <li>- Low attrition and high-quality advisors</li> </ul>
<b>3. Tech Differentiation</b> Uniqueness, defensibility, of the technology.	<ul style="list-style-type: none"> <li>- Proprietary tech (e.g. AI-based threat engine)</li> <li>- Strong integration capabilities (e.g. with AWS, GCP, local infra)</li> <li>- Patent/IP or significant R&amp;D edge</li> </ul>	<b>7. Channel &amp; Partnerships</b> Go-to-market strength via local partnerships	<ul style="list-style-type: none"> <li>- Active partnerships with system integrators or telcos</li> <li>- Strong SEA channel partner strategy</li> <li>- Low CAC via channel leverage</li> </ul>
<b>4. Regulatory Readiness</b> Compliant with local data protection environments	<ul style="list-style-type: none"> <li>- Fully compliant with local laws - Regional certifications (ISO 27001, SOC 2)</li> <li>- Supports localization</li> </ul>	<b>8. Scalability</b> Ability to grow across SEA or globally.	<ul style="list-style-type: none"> <li>- Operations already in 2–3 SEA markets</li> <li>- Modular platform easily customizable per market</li> <li>- Strategy for ASEAN + potential expansion beyond</li> </ul>



**YAMADA  
CONSULTING  
& SPIRE**

### Important Notice

- ▶ The information contained herein is intended to be provided to the client company only for internal use to decide on whether or not to utilize services, and the delivery of the information shall not cause any contract or apply for any contract on any trading or consulting services.
- ▶ No one, including Y&S, shall guarantee or warrant any accuracy, completeness and validity of, and be responsible for any influence of the information contained herein.
- ▶ All rights of information contained herein belong to Y&S. Recipient(s) of this document shall not copy, reproduce, disclose, or distribute to any third party this document and information contained herein without prior written consent of Y&S.

# THANK YOU!

- @ spire@spireresearch.com
- +65 6838 5355
- Yamada Consulting & Spire Pte. Ltd.  
78 Shenton Way #24-01 Singapore 979120
- www.yamada-spire.com

