Kuala Lumpur – 9 December 2025 | Priyesh Pradhan – Senior Underwriter PFR & Cyber

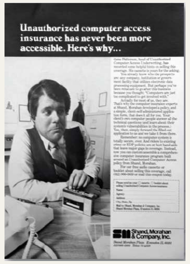
Cyber: Emerging trends, AI and Insurance

MARKEL

Cyber Timeline

1980

Computers take off



Unauthorized computer access insurance has never been more accessible. Here's why...

Gene Patterson, head of Unauthorized Computer Access Underwriting, has recorded some helpful hints on selling this coverage. His cassette is yours for the asking.

You already know who the prospects are: any company, institution or government facility that utilizes electronic data processing equipment. But perhaps you've been reluctant to go after this business because you thought, "Computers are just too complicated to get involved with."

Actually for most of us, they are. That's why the computer insurance experts at Shand, Morahan developed a policy, and a simple, client-self-administered application form, that does it all for you. Your client's own computer people answer all the technical questions (and learn about their system's vulnerabilities in the process.) You, then, simply forward the filled-out application to us and we take it from there.

Remember: no computer system is totally secure, ever. And riders to existing crime or EDP policies are at best band-aids that leave major gaps in coverage. Instead, now you can custom assemble a comprehensive computer insurance program built around an Unauthorized Computer Access policy from Shand, Morahan.

For our free audio cassette or booklet about selling this coverage, call [illegible] or mail this coupon today.

Please send me your □ cassette □ booklet about selling Unauthorized Computer Access insurance.

Name

Agency

Address

City, State, Zip

Mail to: Shand, Morahan & Company, Inc. Shand Morahan Plaza, Evanston IL [illegible]

Shand, Morahan & Company, Inc.

Shand Morahan Plaza Evanston IL [illegible]

[illegible]

1980

The first Tech E&O policies are created

1998

UK Data Protection Act

First Cyber policy written by AIG 1997 / Lloyds 1999

2000

The Dotcom Crash

Y2K

2003

Californian Notification Laws

2008

US Cyber Premiums estimated to be $500m.

PCI Breaches

2013

The Global Cyber product arrives.

Target breach in US

2024

Estimated 5bn internet users.

Over 150 Cyber Insurers

PP1

Cyber Security threats evolution

2020

- Malware
- Phishing
- Spear phishing
- Man in the middle attack
- Denial of service attack
- Ransomware
- Zero-day exploit
- Advanced persistent threat

2025

- Social engineering
- AI powered attacks
- Quantum computing threats
- RAAS
- Cloud vulnerabilities
- Data breach vulnerabilities
- IoT devices threats
- Configuration errors/threats
- Supply chain vulnerabilities

Sources: ipwithease.com | stealthlabs.com

Slide 3

PP1	[@Mukasa, Etta] , I have changed to this slide. However I was not able to add design co-pilot to this slide. Can you help in this? Pradhan, Priyesh, 2025-12-02T17:01:10.314
EM1 0	I’ll get back to this slide on Friday [@Pradhan, Priyesh] [@Polston, Megan] Mukasa, Etta, 2025-12-02T17:29:26.619

Cyber & Physical Damage (CZ)

- Ukraine Power Stations
- German Smelter Plants
- Stuxnet Iranian Power
- Turkish Pipelines
- Saudi Arabia Drone Attack

AI in cyber space

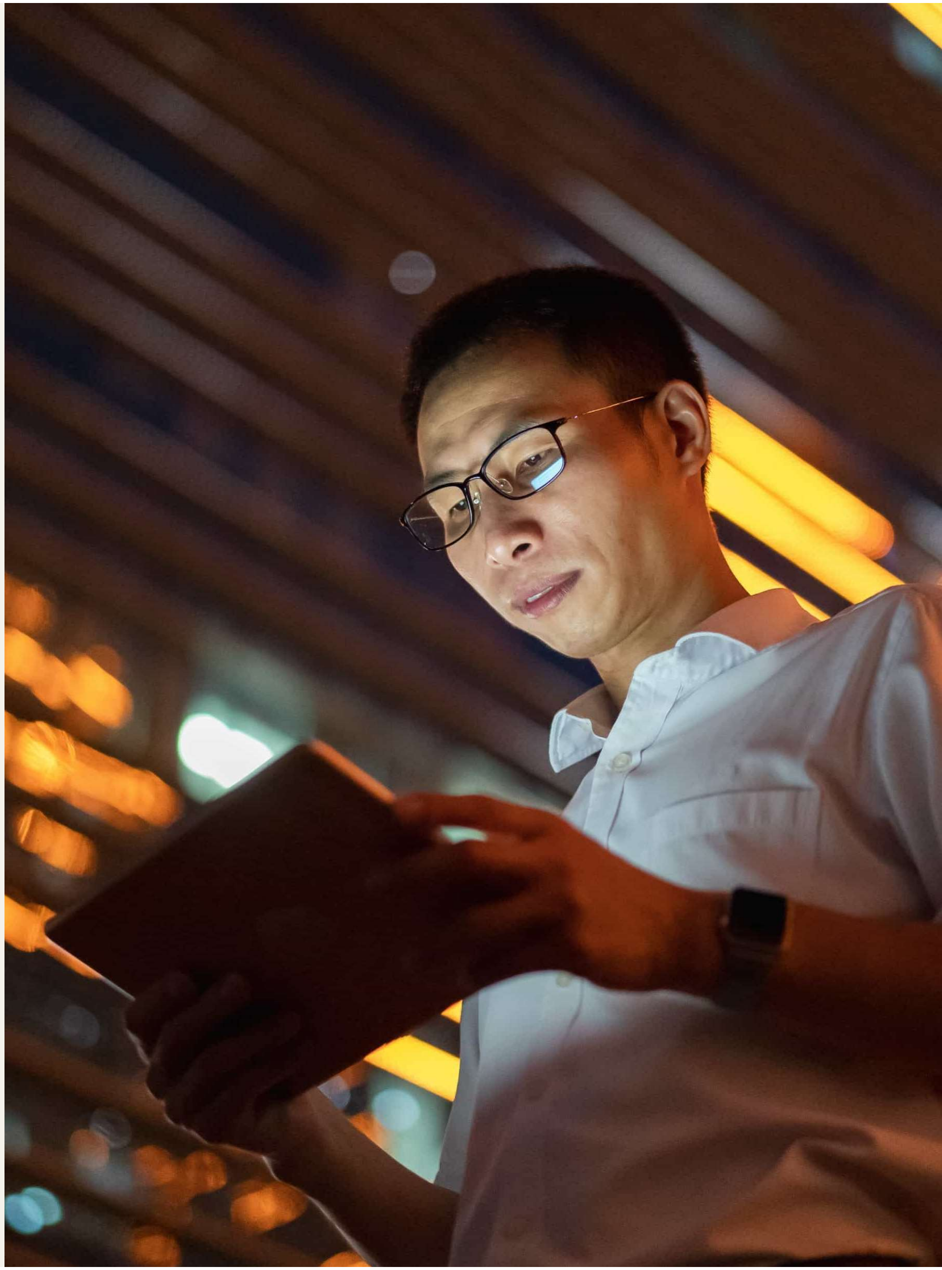
AI – Double Edged Sword?

Adoption of AI in Organisations

- 80% of organizations use AI in critical operations
- Companies using it to improve efficiency
- Companies using it to a limited extent, appointing third parties to do so
- Companies creating AI themselves

Risks and Opportunities of AI

- With great data comes great exposure
- AI amplifies speed, scale, and sophistication, for both innovation and attacks
- AI creates new value and new vulnerabilities
- AI is not the enemy of risk — it's the evolution of it
- Design resilience as smart as the systems we build



Introduction to Cyber Risk in the AI Era

Evolution of Cyber Threats

AI has transformed traditional cyber threats by introducing new sophisticated attack methods.

Dual Role of AI

AI acts both as a cybersecurity defender and as a tool for attackers to launch complex attacks.

AI-Powered Cyber Attacks

Examples include AI-generated phishing, deepfake videos, and adaptive autonomous malware.

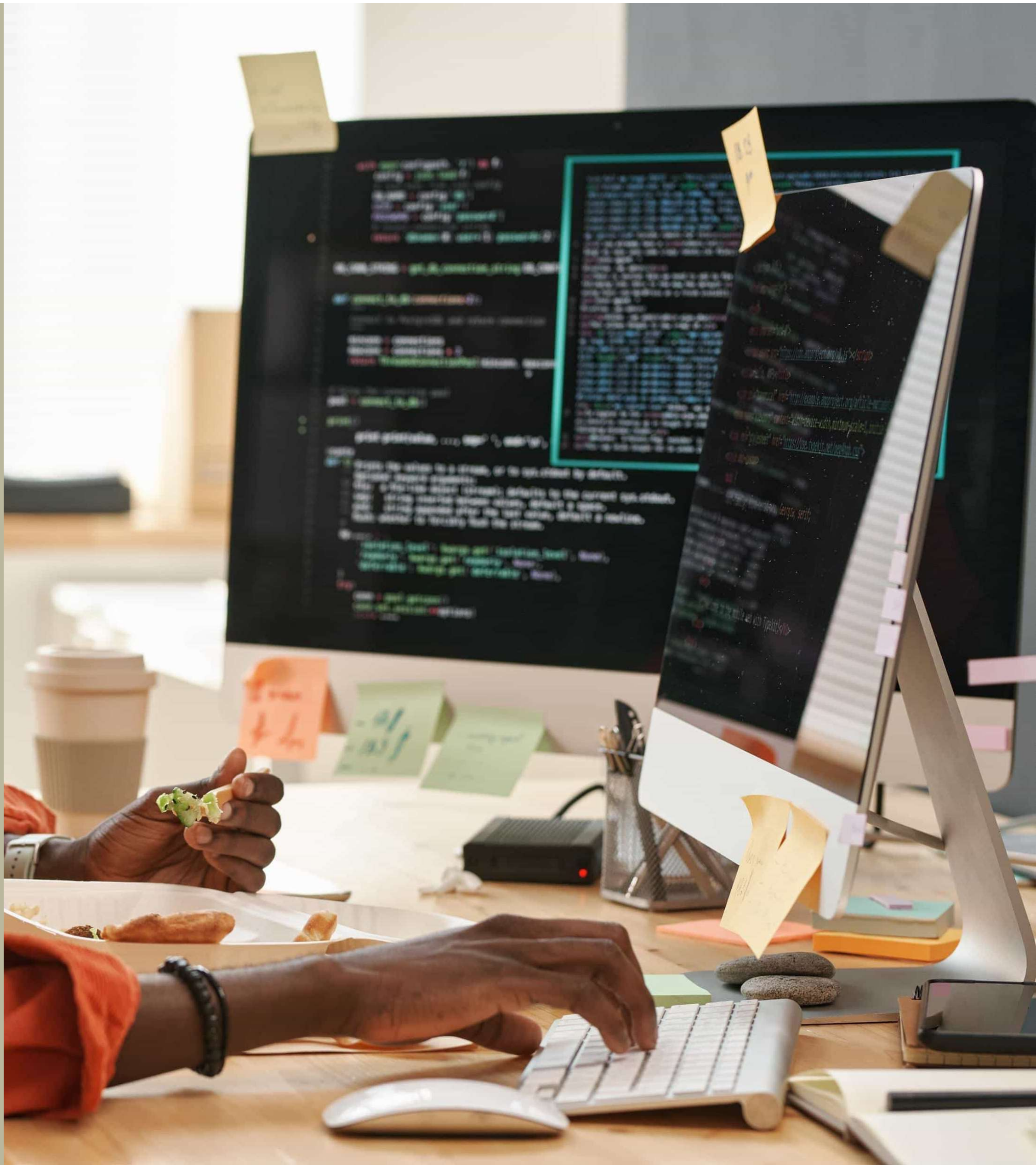
Strategic Risk Management

Organisations must address AI-driven cyber risks as a keyboard-level strategic concern.

Data Poisoning – Model manipulation

Deliberate attempt to bias an AI model's training data

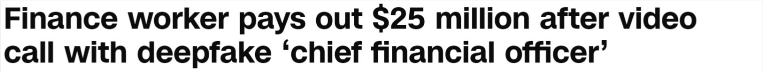
Dirty Data



Types of Cyber risk

- **System Failure Outage:** A system failure or technical glitch that leads to downtime of application or service
- **AI and Emerging Risk:** Due to the advancement of AI, new tools and threats have merged

AI Powered Phishing Tools

- **DeepPhish:** AI-driven tools that generate highly convincing phishing emails by mimicking the target's communication style and content.
- **Spear Phishing Generators:** These tools use AI to create personalized phishing messages aimed at specific individuals, increasing the likelihood of a successful attack
- **HK:** 

  Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

AI Malware

- **AI-Driven Malware:** Malware that uses AI to evade detection by dynamically changing its behavior or appearance. This type of malware can learn to bypass traditional security systems
- **Tech PI Consideration:** use of generative AI may lead to an increase in E&O

Global Regulation & Legislation Growth

- **GDPR:** UK & Europe
- **EU:** 9th Dec 2023 EU Artificial Intelligence Act
- **DORA:** Digital Operational Resilience Act 16/01/2023 and 17/01/2025
- **US:** CCPA, HIPPA, COPPA, BIPA
- **India:** Personal Data Protection Bill
- **Brazil:** LGPD
- **Canada:** PIPEDA
- **South Africa:** Protection of Personal Information Act (POPI)

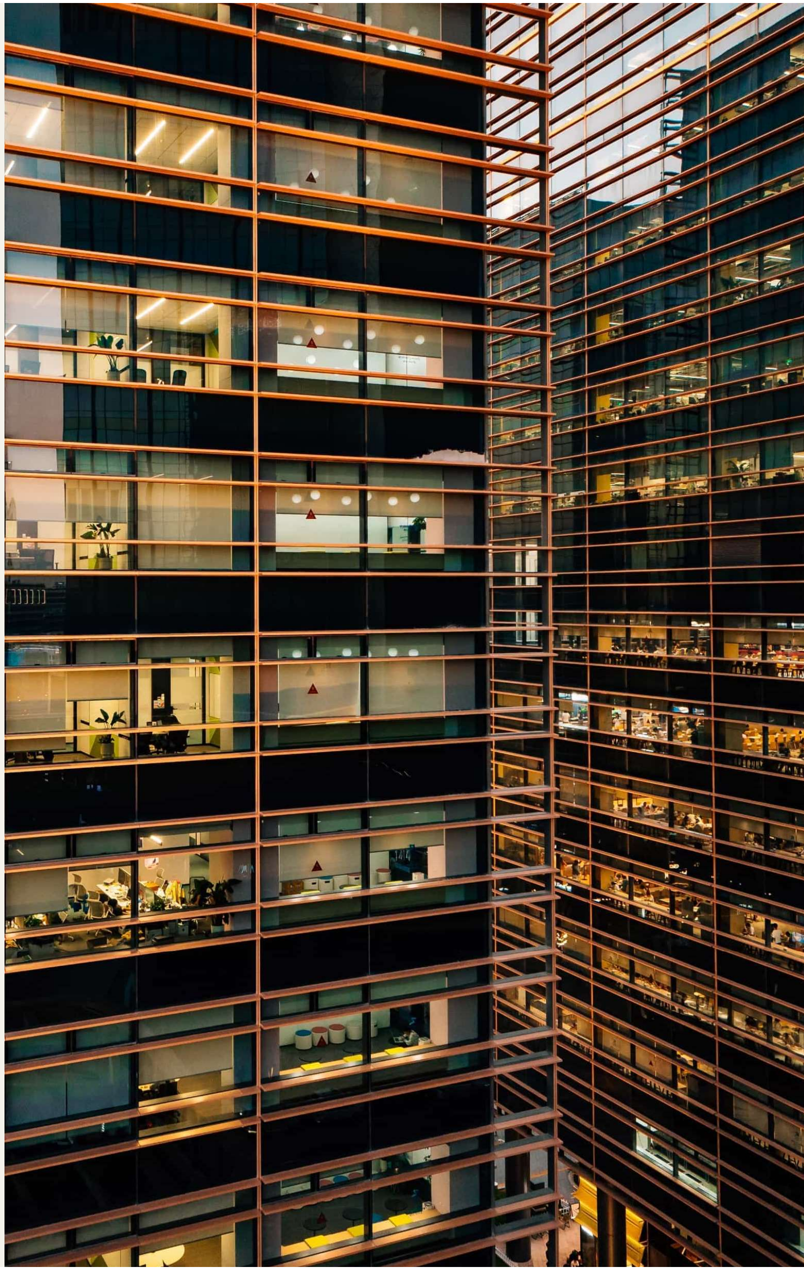
GDPR Enforcement

1. Meta Platforms Ireland €1.2bn (2023)
2. Amazon Europe €746m (2021)
3. Meta Platforms Inc €405m (2022)
4. Meta Platforms Ireland €390m (2023)
5. Tik Tok Ltd €345m (2023)
6. Meta Platforms Ireland €265m (2022)
7. WhatsApp Ireland €225m (2021)
8. Google Inc €50m (2019)
9. Criteo €40m (2023)
10. H&M €35.3m (2020)
11. TIM €27.8m (2020)
12. British Airways €22m (2020)
13. Clearview AI Inc €20m (2022)
14. Marriott Int €20m (2020)
15. Meta Platforms Ireland €17m (2022)
16. Wind Tre €16.7m (2020)
17. Deutsche Wohnen €14.5m (2019)
18. Tik Tok €12.7m (2023)
19. Vodafone Italia €12.25m (2020)
20. Eni Gas e Luce €11.5m (2020)

Source: Skillcast April 2024

Data Privacy Laws – Asia Pacific

- **Singapore:** Personal Data Protection Act 2012 (2020 Revised Edition) (PDPA)
- **Malaysia:** Personal Data Protection Act 2010 (PDPA)
- **India:** Digital Personal Data Protection Act
- **Hong Kong:** The Personal Data (Privacy) Ordinance (PDPO)
- **Thailand:** Personal Data Protection Act 2019 (PDPA)
- **People's Republic of China:** Personal Information Protection Law
- **Japan:** The Act on the Protection of Personal Information (2003)
- **Republic of Korea:** Personal Information Protection Act (PIPA)
- **Philippines:** Data Privacy Act 2012 (DPA)
- **Taiwan:** Personal Data Protection Act (PDPA).
- **Vietnam:** Decree on Personal Data Protection (Decree)
- **Australia:** The Australia Privacy Act



Cyber risks – Malaysia

83%

Surge in scam calls

↑

29%

Data breaches

71%

Phishing led fraud cases

↑

153%

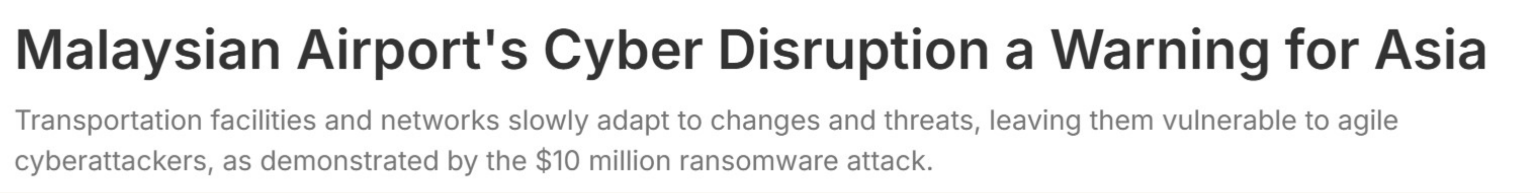
Ransomware incidents

Top 5 Cyber Security risks in Malaysia:

- Ransomware attacks on critical infrastructure
- Quishing
- API vulnerabilities in financial services
- Data breaches
- Attacks by cyber groups

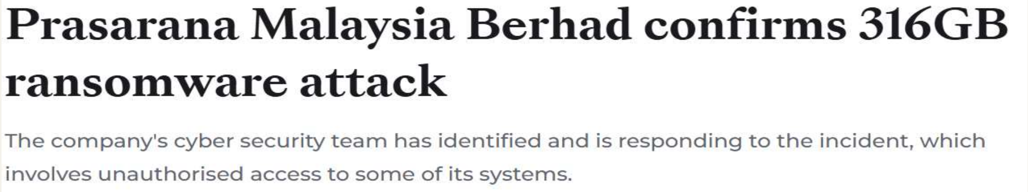
Source: https://securityquotient.io/

Malaysia Cyber Attacks



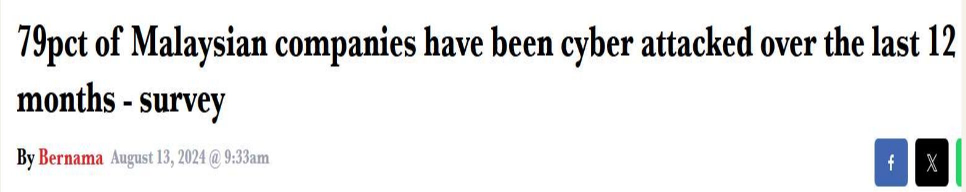
Malaysian Airport's Cyber Disruption a Warning for Asia

Transportation facilities and networks slowly adapt to changes and threats, leaving them vulnerable to agile cyberattackers, as demonstrated by the $10 million ransomware attack.



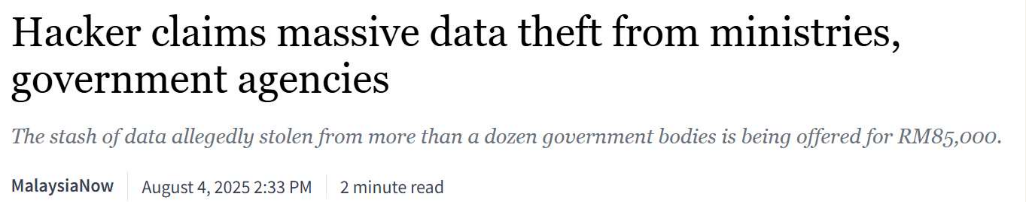
Prasarana Malaysia Berhad confirms 316GB ransomware attack

The company's cyber security team has identified and is responding to the incident, which involves unauthorised access to some of its systems.



79pct of Malaysian companies have been cyber attacked over the last 12 months - survey

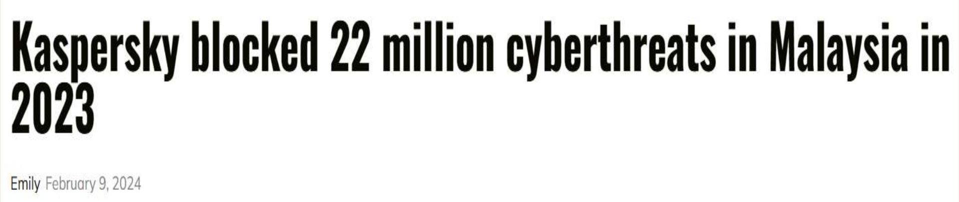
By Bernama August 13, 2024 @ 9:33am



Hacker claims massive data theft from ministries, government agencies

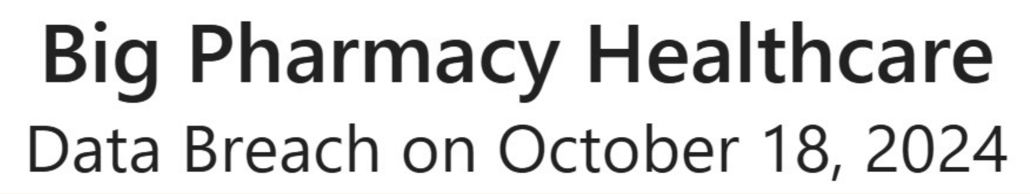
The stash of data allegedly stolen from more than a dozen government bodies is being offered for RM85,000.

MalaysiaNow | August 4, 2025 2:33 PM | 2 minute read



Kaspersky blocked 22 million cyberthreats in Malaysia in 2023

Emily February 9, 2024



Big Pharmacy Healthcare

Data Breach on October 18, 2024

Source:

breachsense.com

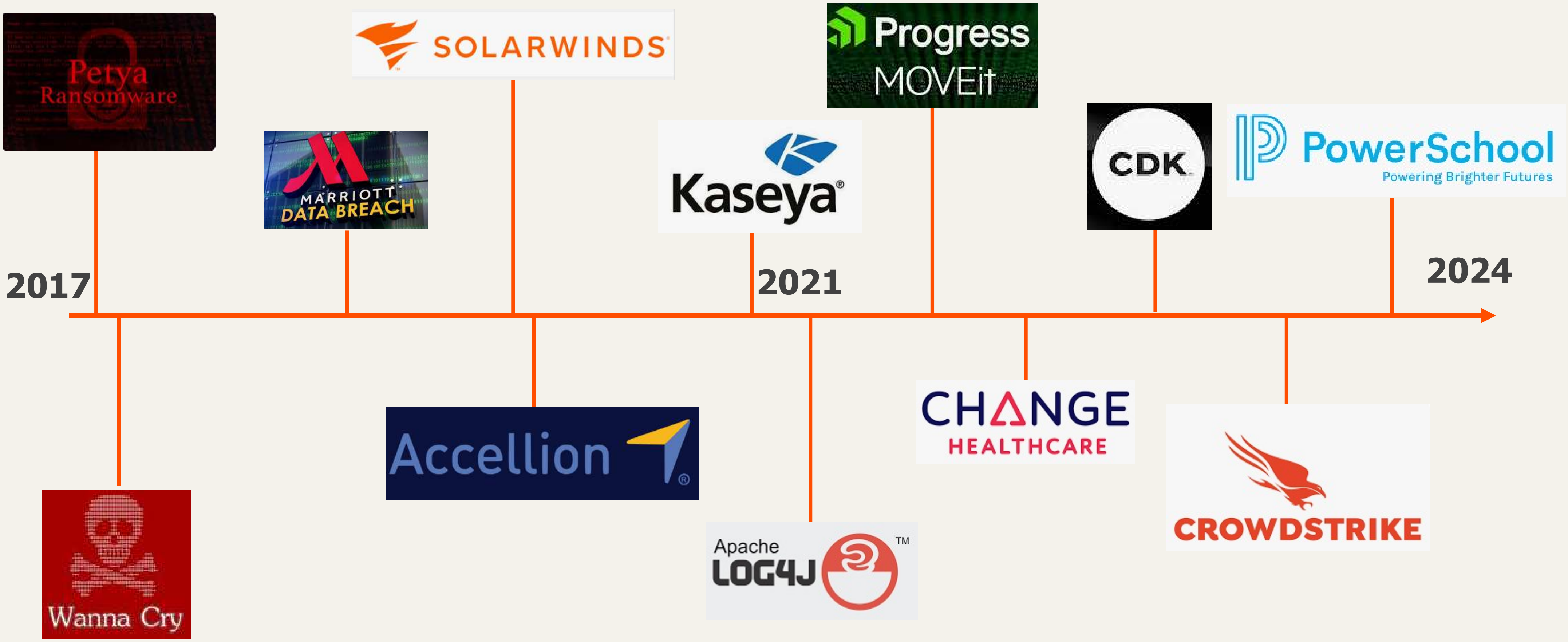
Kaspersky www.darkreading.com
Malaysianow https://ciosea.economictimes.indiatimes.com/

Factors Contributing to the Vulnerability of Malaysian Businesses

- Human Error
- Legacy systems
- Resource limitations
- Rapid digital transformations
- Regulatory complexity
- Sophisticated cyber attacks

Cyber claims

Major Cyber Events & Widespread Events timeline



2017

2021

2024

Claim Scenario – MGM

MGM owns 24 hotels and locations

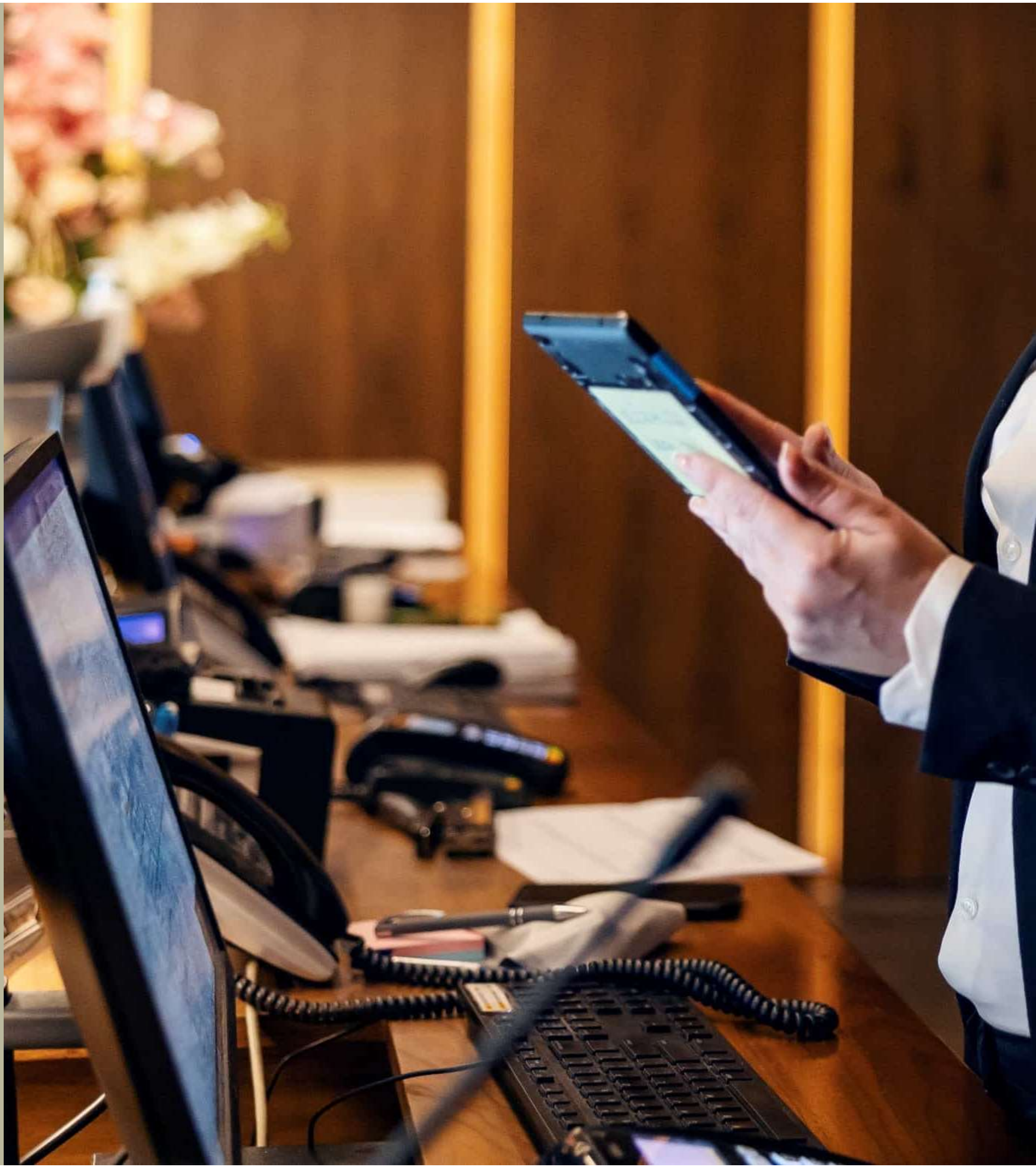
10 days of downtime incurred

What was impacted:

- Hotel guest were unable to check-in
- Hotel rooms and digital cards would not allow guest to check in
- Slot machines seized functioning
- 6 Terabytes were stolen
- Payroll systems were impacted

In addition to the $100 million loss from **business disruptions,** MGM said it also incurred less than $10 million in one-time expenses, which included technology **consulting services, legal fees** and expenses of other third-party advisors.

Several weeks later MGM provided another update with some bad news for its guests: The hackers were able to access their personal information, including names, contact information, gender, date of birth, driver's license, passport, and even Social Security numbers, from "some customers" before March 2019.



Claim Scenario – Marks & Spencer

Incident

- Major cyberattack disrupted online sales & contactless payments for 3+ weeks.
- Personal data accessed (non-financial).
- Estimated claim: **£10m – £100m** (Allianz & Beazley, Willis XS Facility).

Key Coverages Triggered

- **Business Interruption** – £40m+ lost online sales, extra expenses.
- **Breach Response** – forensics, legal, PR, customer notification.
- **Privacy Liability / Regulatory** – potential claims & investigations.
- **(Cyber Extortion)** – no evidence of ransom demand.
- **(Contingent BI)** – no supply chain disruption reported.

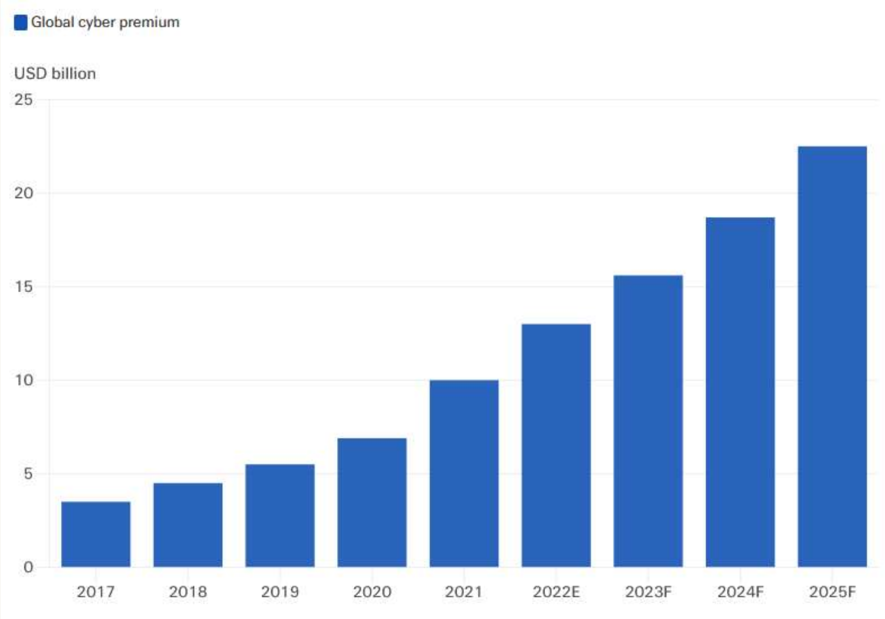
Market Impact

- Retail cyber premiums up ~10% post-incident.
- Heightened underwriting scrutiny for UK retailers.

Insurance

Cyber Market Growth

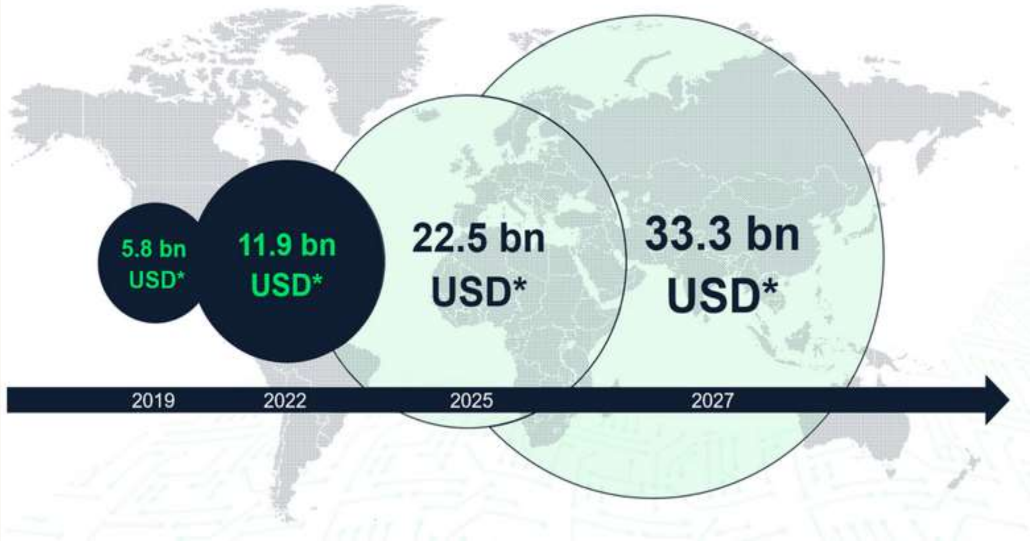
- UK Cyber Market Value – **$2bn est.**
- European Cyber Market Value – **$1.5bn est.**
- US Cyber Market Value – **$10bn est.**



Source: Swiss Re Institute
Note: E=Estimates, F=Forecasts. Swiss Re estimates/forecasts comprise standalone and packaged cyber policies.

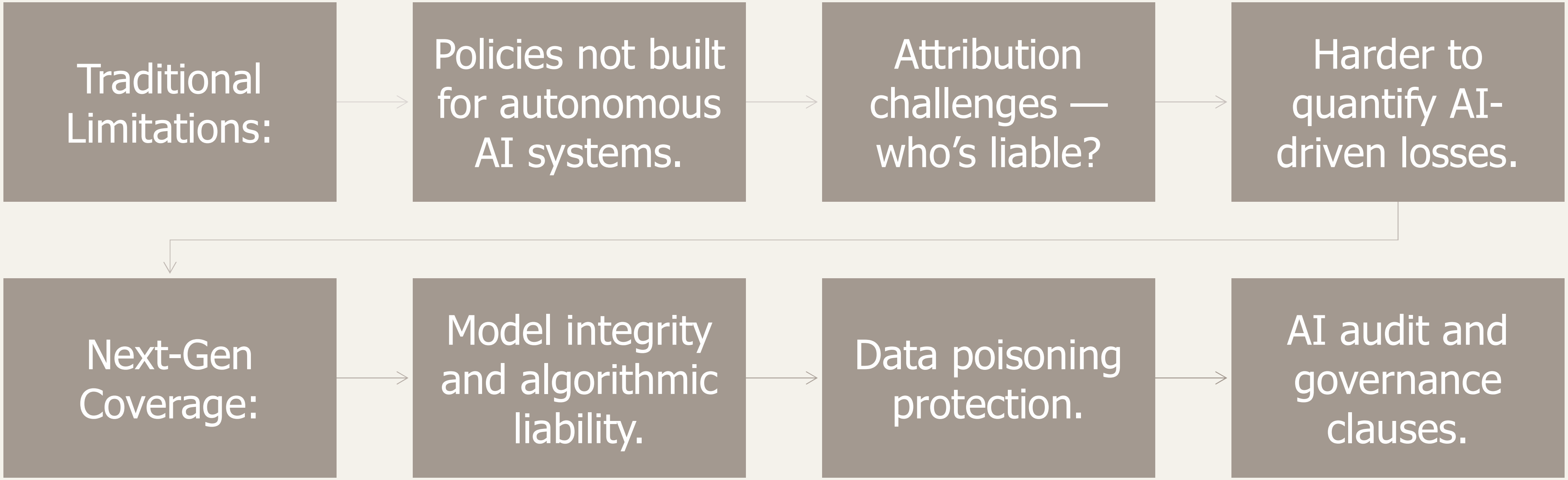
Global cyber insurance market: Demand continues to grow

*Estimates by Munich Re



Sources:
- Swiss Re What you need to know about the Cyber insurance market 28 Aug 2023
- Munich Re, Cyber Insurance Risks and Trends 2024

Rethinking Cyber Insurance



Traditional Limitations:

Policies not built for autonomous AI systems.

Attribution challenges — who’s liable?

Harder to quantify AI-driven losses.

Next-Gen Coverage:

Model integrity and algorithmic liability.

Data poisoning protection.

AI audit and governance clauses.

What strategies might a Risk Manager employ?

1. **Assess AI exposure**
   find where AI touches critical assets.

2. **Align governance**
   merge cybersecurity with AI ethics.

3. **Engage early with insurers**
   build AI-risk transparency.

4. **Simulate AI incidents**
   red team your models.

5. **Managing AI risk isn’t about fear**
   it’s about foresight.

Cyber 360 offering

Cyber and Privacy Liability	Regulatory Investigations & Fines	E-media Liability
Privacy Breach Notification & Mitigation Costs	Business Interruption	Extortion costs & Cyber theft

Markel Cyber 360 – Coverage

Cyber Liability & Loss

- Cyber & Privacy Liability
- Privacy Breach Notification and Mitigation Costs
- Business Interruption:
- Malicious Cyber BI
- Dependent BI
- System Failure BI
- Dependent System Failure BI
- PCI Fines and Regulatory Investigations
- Extortion

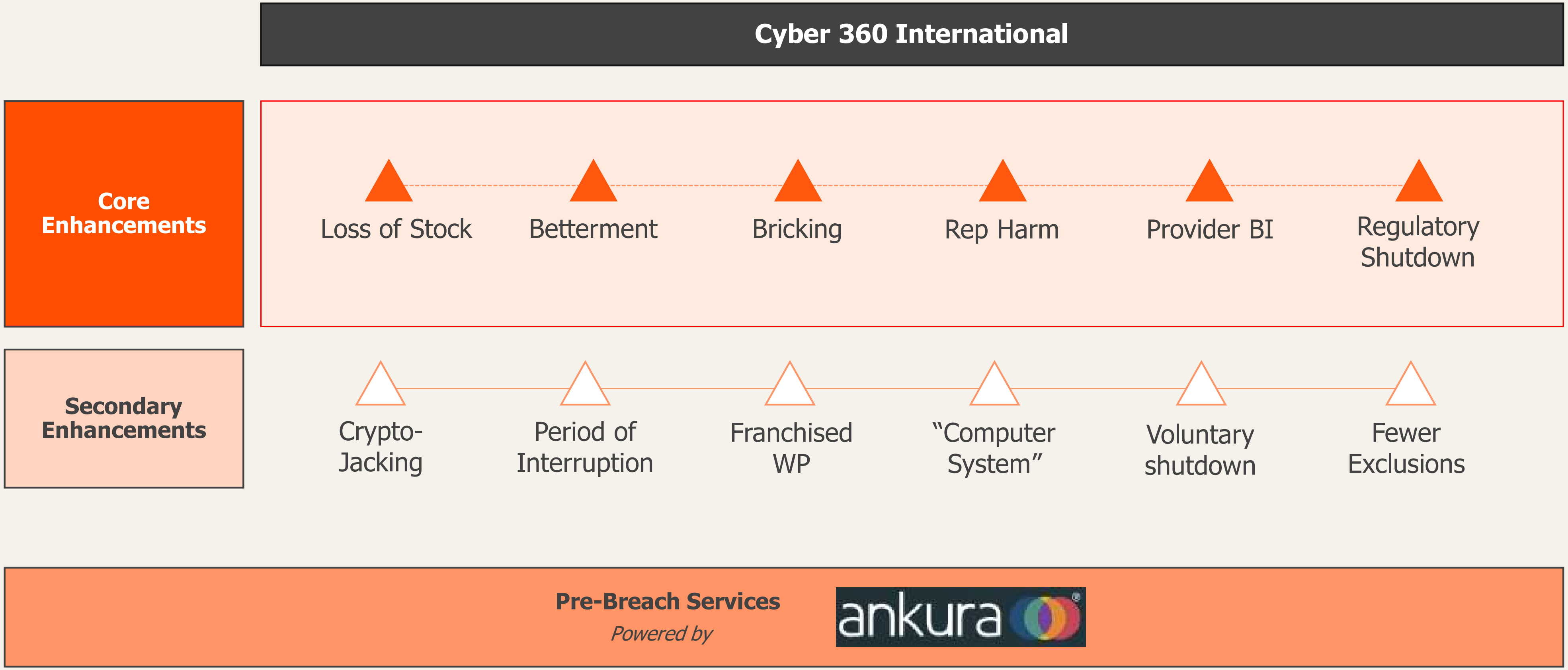
Extensions

- Acquisitions & Formations of Companies/Subsidiaries
- Additional Limit for Non-Execs
- Extended Reporting Period
- Mitigation Costs

Cyber

- Reward Coverage
- Betterment
- Voluntary Shutdown
- Regulatory Shutdown
- Telecomm Fraud
- Crypto-Jacking

Cyber 360 offering



Cyber 360 International

Core Enhancements

- Loss of Stock
- Betterment
- Bricking
- Rep Harm
- Provider BI
- Regulatory Shutdown

Secondary Enhancements

- Crypto-Jacking
- Period of Interruption
- Franchised WP
- “Computer System”
- Voluntary shutdown
- Fewer Exclusions

Pre-Breach Services

Powered by ankura

MARKEL