



Cyber Risk and Insurance Information Session

Institute of Chartered Shipbrokers, Singapore Branch

Presented by Willis, a WTW company
with support from S-RM

10 March 2025

Agenda

Part 1 - Overview – Cyber risks facing the maritime sector

Part 2 – Ransomware/Cyberattack - Live Simulation

Part 3 – Practical steps to improve Cyber Risk Management

Part 4 - Cyber Insurance – Overview and Benefits

Overview – Cyber risks facing the maritime sector in 2025

Broad Cyber Risks

Evolving perimeter:

- Constant evolution
- Increasingly fragmented and complex systems and security stacks

System vulnerabilities:

- Direct Losses
- Loss of Revenue
- Financial Burden

Ransomware:

- Incident Response and extortion negotiation support

Data Exposure:

- More stringent data privacy regimes

Maritime Sector-specific

Supply Chain:

- Supply Chain Vulnerabilities
- IT/Non-IT Provider Exposure

Reputational Risks:

- Brand Damage
- Trust Erosion
- Reputation Fallout

Business Interruption:

- Costs associated with wrongful loss of cargo failure to deliver

Compliance with Maritime Cybersecurity regulatory regimes:

- Investigation costs from regulatory bodies into non-compliance

Maritime forecasted security trends in 2025

AI-enabled threats; increasingly sophisticated exploits that can evade traditional detection methods

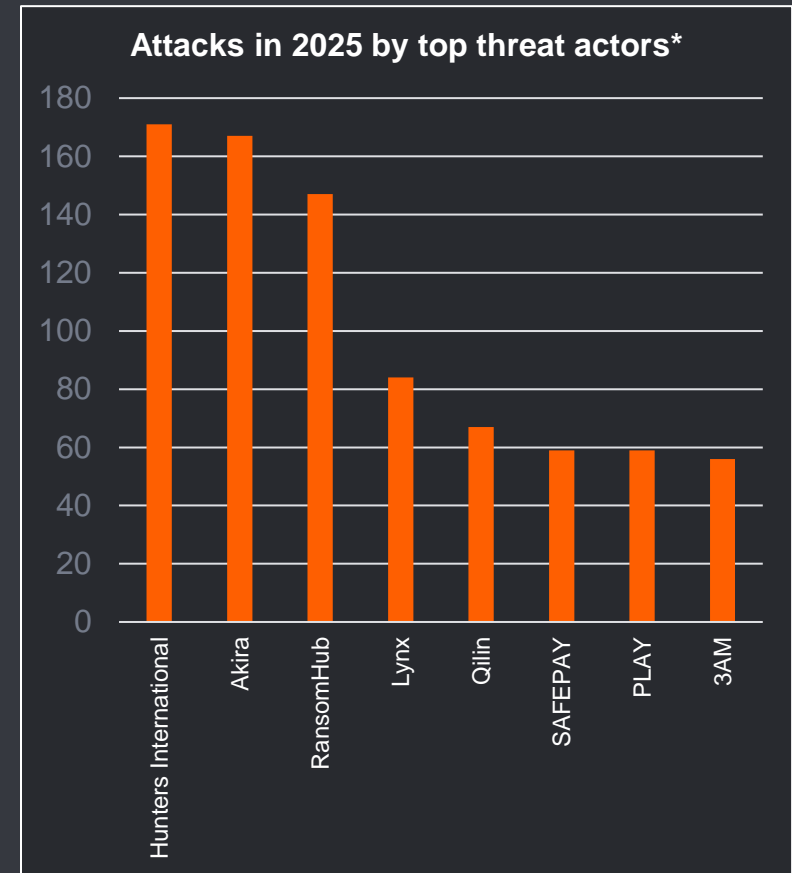
Interconnectivity of maritime operations present multiple points of vulnerability; supply chain attacks mounting in concern

Operational Technology (OT) vulnerabilities: systems which govern essential shipboard functions often rely on outdated software

Increasing adoption of autonomous systems and automation risks – automated port operations bring in new vulnerabilities.

Threat Landscape

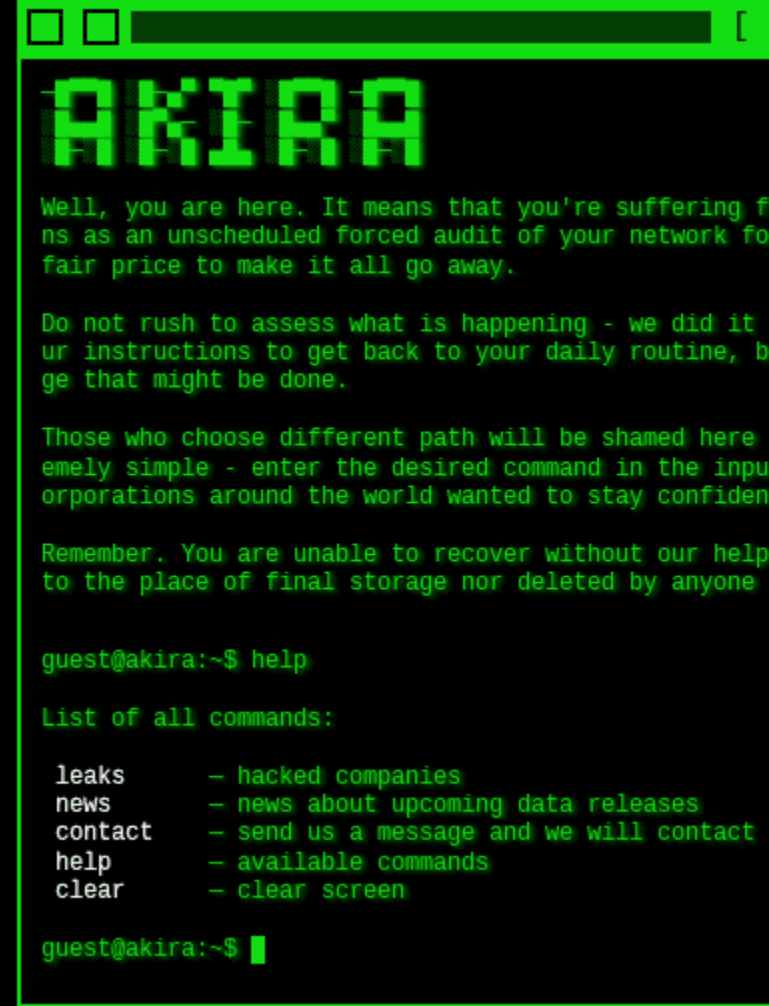
- Ransomware gangs have **compromised over 1,400 companies** so far this year.
- **Over two-thirds of these companies have had data exposed** as part of these attacks.
- The majority of these companies have their headquarters in North America. Approximately **15% of these companies are based in APAC**.
- The threat actors with the most known attacks on companies are **Hunters International, Akira and RansomHub**.
- In July 2023, the **Port of Nagoya** was hit by the LockBit 3.0 ransomware group, **causing the port to halt cargo loading operations** while dealing with the attack.



*Data based on victim's posted to the actor's leak site, and thus unlikely to be comprehensive of all victims.

S-RM Threat Intelligence

- First identified in March 2023 and a suspected Russian cybercrime group
- Akira operates a Ransomware-as-a-Service ('RaaS') model. Affiliates purchase access to the ransomware by paying 20% of any ransom paid to the developers/managers.
- Akira have named 633 victims on their dedicated dark web leak site to date.
- There is no free decryptor which works for the current version of Akira ransomware



```
AKIRA

Well, you are here. It means that you're suffering from ransomware. We have access to your data. We will send you the data as an unscheduled forced audit of your network for a fair price to make it all go away.

Do not rush to assess what is happening - we did it for your instructions to get back to your daily routine, but we will get that might be done.

Those who choose different path will be shamed here. It is very simple - enter the desired command in the input field. We will be happy to see the corporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. The data is not in the place of final storage nor deleted by anyone.

guest@akira:~$ help

List of all commands:

leaks      - hacked companies
news       - news about upcoming data releases
contact    - send us a message and we will contact you
help       - available commands
clear      - clear screen

guest@akira:~$ █
```

Can you trust criminals?

Organised ransomware business models go after long-term revenues from many victims, which means they must establish a level of “trustworthiness” by honouring agreements.

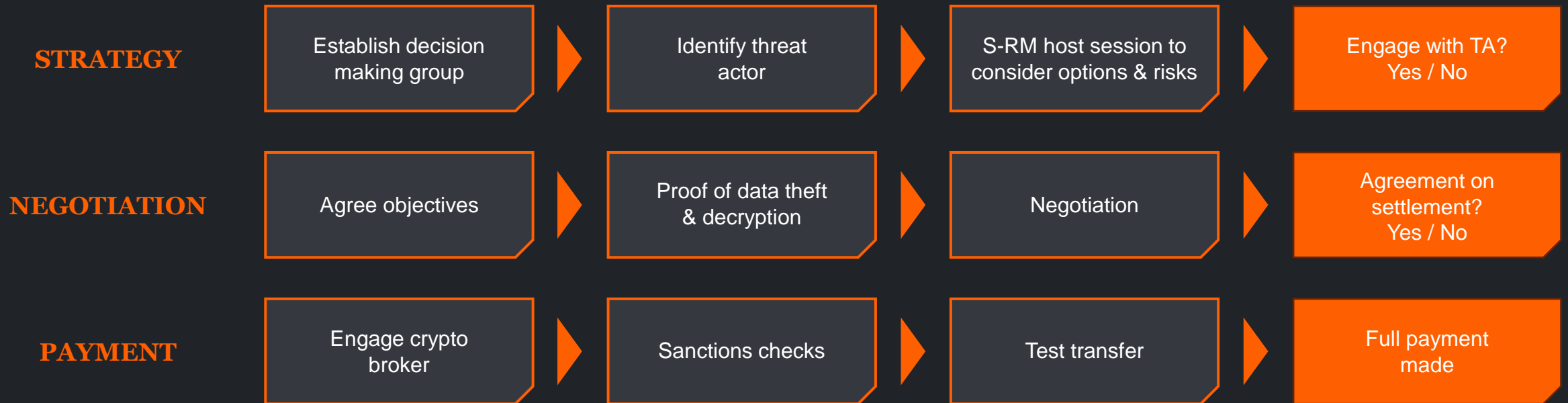
Proof of possession and decryption and stolen data has become a common and relatively frictionless process that is accepted by most prolific ransomware group

Staging payments with ransomware groups rarely works or is accepted.

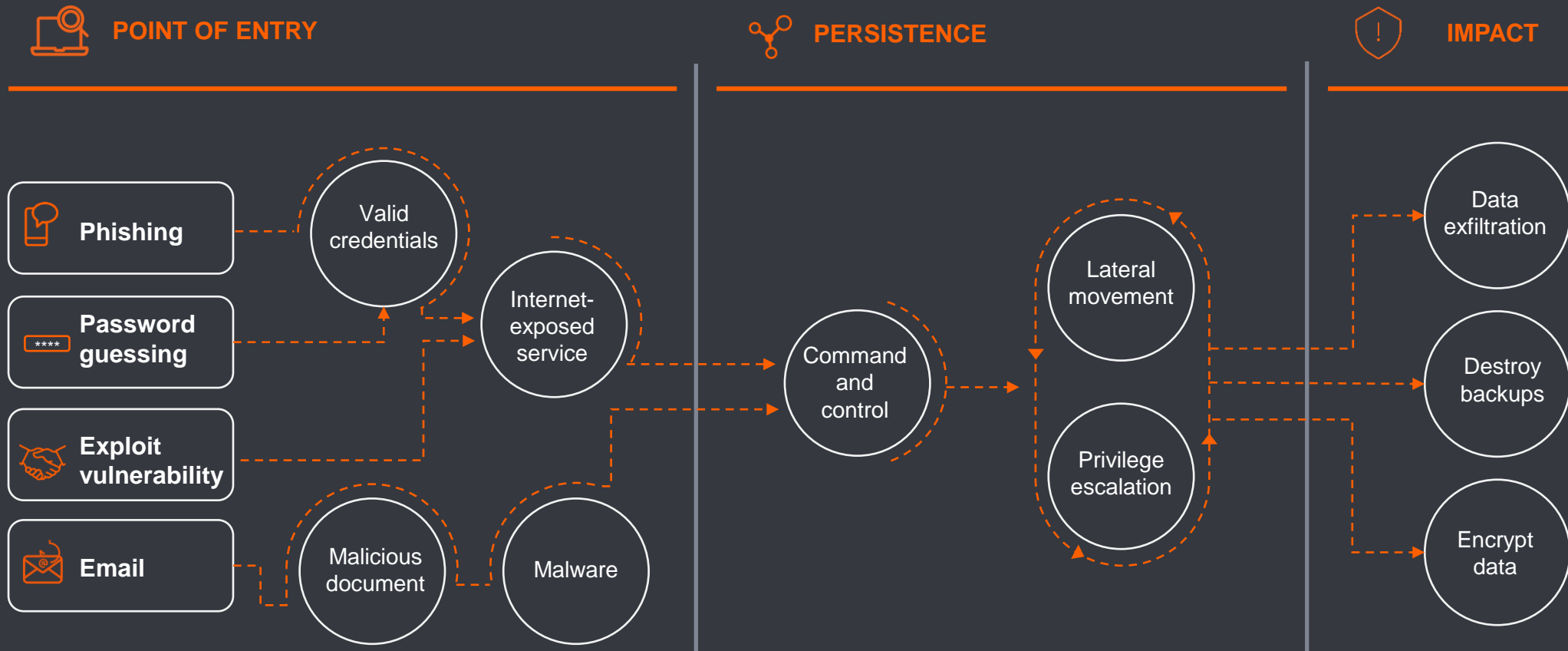


Negotiation process

While each negotiation is unique, in most cases the negotiation will involve the following steps.



Investigating the Incident Lifecycle



Third party coordination

	Legal counsel	Digital forensics	Negotiators	PR & Comms	Forensic accountants	Crypto broker
Involvement Likelihood	High	High	Medium	Medium	Insignificant	Low
Services	<ul style="list-style-type: none"> • Advise on data protection • Regulatory support • Third party contracts • Sanctions and legal advice related to negotiations • Advice related to law enforcement engagement • Litigation support 	Collect, process and analyse data to identify: <ul style="list-style-type: none"> • Point of Entry • Persistence • Defence evasion • Data exfiltration 	<ul style="list-style-type: none"> • Provide intelligence on the extortionist • Walkthrough risks of engagement • Develop negotiation strategy • Communicate with extortionist • Reach final settlement • Provide pre- and post-payment documentation 	<ul style="list-style-type: none"> • Overall strategy for PR and comms throughout the response • Initial internal comms for employees • Comms for clients and customers • Public facing comms for website / public statements 	<ul style="list-style-type: none"> • Financial impact assessment • Business interruption analysis • Support on financial reporting and disclosure during a crisis 	<ul style="list-style-type: none"> • Conduct sanctions check on threat actor • Acquire cryptocurrency prior to payment • Facilitate test payment to threat actor • Facilitate final payment to threat actor • Pay ransom upfront, to be reimbursed later
Instruction phase	Immediately	Immediately	Within first 48-72 hours	Within first 48-72 hours	Within first 72-96 hours	Within 4-7 days

Key takeaways

1. The **profile of your adversary** is crucial for making correct decisions.

2. Accurate **threat intelligence** influences response and negotiation strategy.

3. Paying a ransom involves a consideration of **financial, legal, regulatory, reputational** and **ethical** concerns.

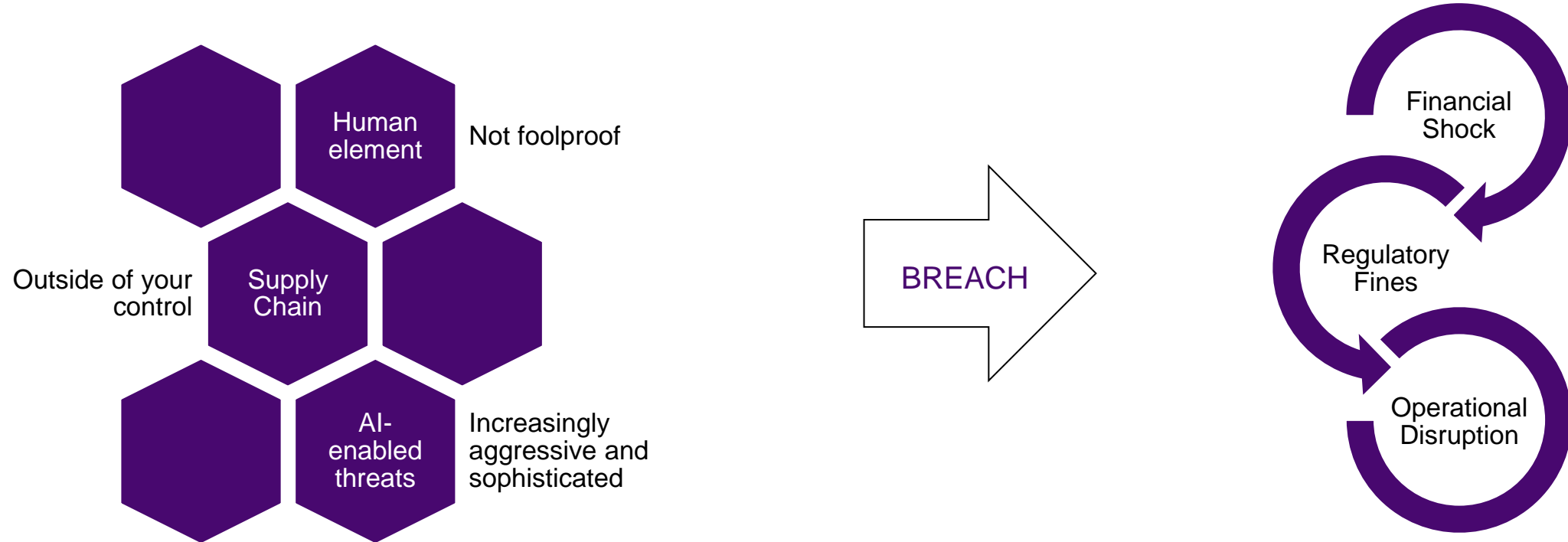
4. Establish **how you would pay a ransom** before an incident to reduce the number of decisions needed.

5. Take legal advice to ensure your cost benefit analysis of a potential payment is the full picture. Remember, **you might still need to notify affected people if you pay.**

6. Above all, **engage with experts** as early as possible to feed into all phases of the response.

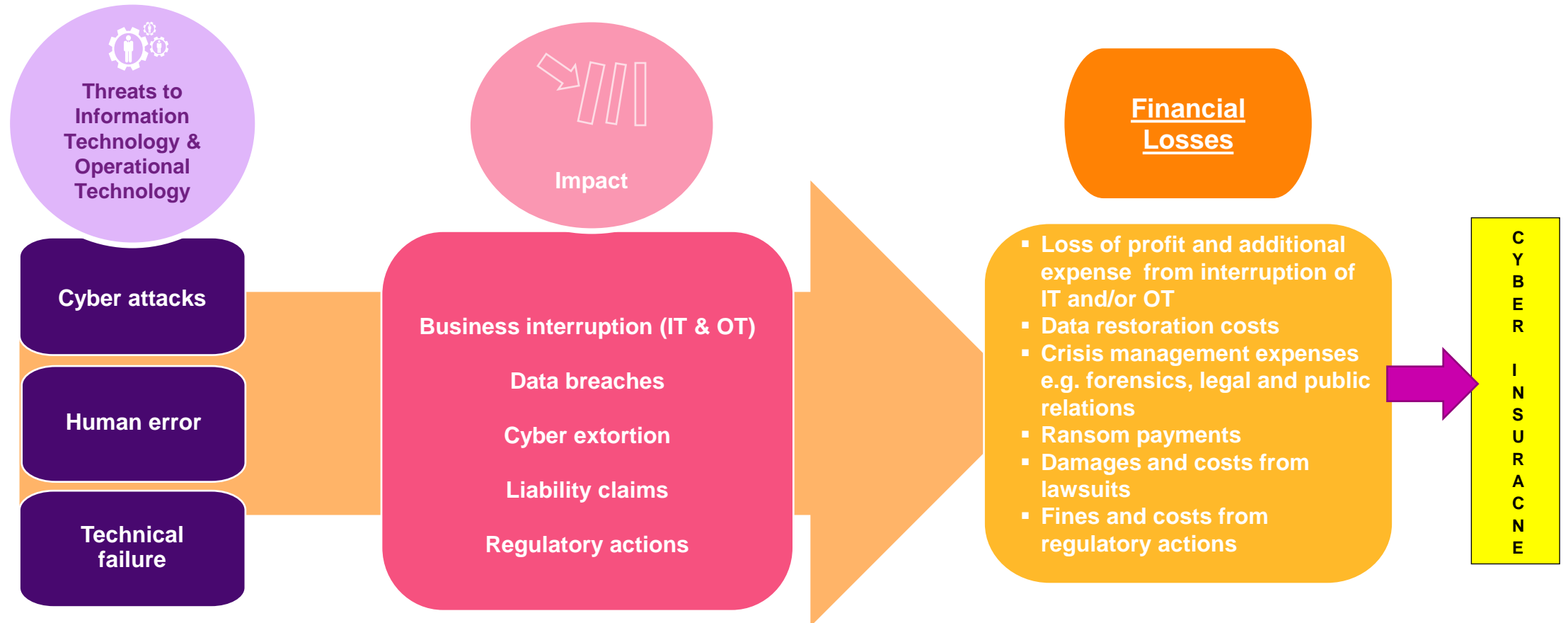
Cyber Risk – Not an IT issue

The Board is responsible for the risk management, financial performance, regulatory compliance, operational continuity and overall reputational protection of the company. **Cyber risk cuts across each of these facets.** While frontline defense must be prioritized, no security can be 100%.



Cyber insurance is part of a cross-functional business strategy rather than a security issue or IT expenditure

What is Cyber Insurance in a nutshell?



Benefits of a Cyber Insurance Policy

A critical element of a comprehensive cyber risk management strategy

Immediate Incident Response Assistance

- 24/7 crisis hotline
- \$0 Retainer for Crisis Response Experts: readily available panel of digital forensics investigators, crisis specialists, legal counsel and PR firms

Costs of external investigators Covered

- Costs of external investigators is rising due to shortage of supply and exponential increase in demand.
- Costs can quickly escalate to seven-digit figures

Costs to restore systems and business interruption covered

- Costs to restore or recreate data can escalate, depending on the severity of malware.
- Backups are not always reliable
- Business downtime can span weeks or months, depending on the severity of the malware

Loss Data – Based on Willis Cyber portfolio

Loss trends 2021-2023

Components	Trend	Median (USD)	Mean (USD)
Ransomware Negotiation and Payment	▲ Increasing	\$1,027,205	\$2,676,815
Fines and Penalties	▲ Increasing	\$1,010,810	\$20,210,630
Loss of Profits	▲ Increasing	\$907,050	\$6,620,000
Forensic Costs	▲ Increasing	\$600,050	\$11,340,810
Settlement Costs	▶ Stable	\$217,810	\$508,635
Crisis Management Costs	▲ Increasing	\$190,375	\$513,915
ID Theft Protection	▲ Increasing	\$161,180	\$4,735,030
Defence Costs	▶ Stable	\$112,325	\$952,870
Data Restorations	▲ Increasing	\$178,210	\$2,350,115
Legal Advisory Costs	▲ Increasing	\$124,560	\$721,289
Regulatory Notification Costs	▲ Increasing	\$43,420	\$377,351
PR and Communication Costs	▲ Increasing	\$43,385	\$247,303
Equipment and Hardware Replacement	▼ Reducing	\$40,992	\$199,085
Call Centre Costs	▶ Stable	\$25,918	\$1,456,835
Credit Monitoring	▼ Reducing	\$14,293	\$2,282,160

Willis' CyCore Asia

Introducing CyCore Asia – WTW's bespoke primary Cyber insurance solution

CyCore Asia is a Cyber facility, offering up to USD15m in primary limit to Willis clients across Singapore and Hong Kong.

What value can CyCore Asia bring to you?



Restore function

In the event of a loss, CyCore Asia offers the ability to 'restore' your limit, ensuring you don't spend any time off cover.



Risk bursary

Through CyCore, you will be eligible for cyber risk management services, paid for by insurers and provided by **S-RM** – a specialist cyber security consultancy firm.



Proprietary wording

Leveraging industry expertise, CyCore Asia's proprietary wording provides comprehensive general cyber coverage to help minimise and manage risk effectively.

Restore function

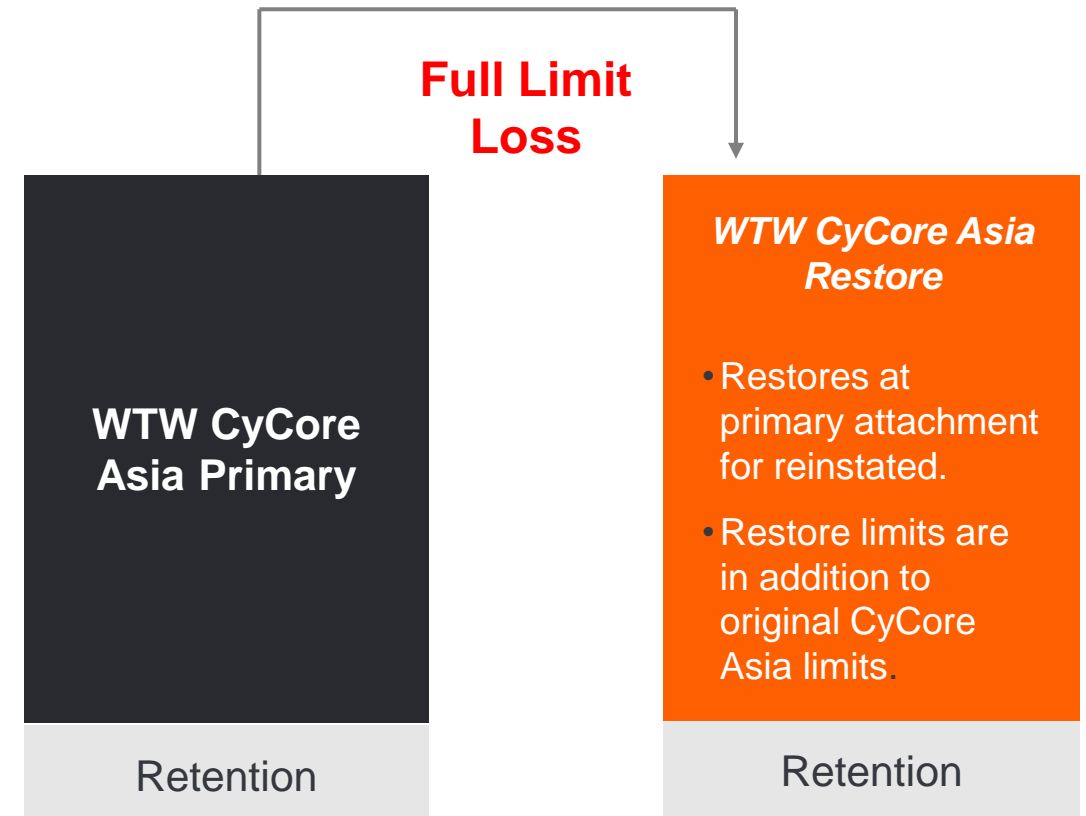


How does the CyCore Asia Restore function work?

- Primary CyCore Asia Capacity – up to USD15m
- If your business suffers a full limit loss, you can ‘restore’ your CyCore Asia capacity at a pre-agreed price, ensuring you are not left off cover

Benefits include:

- Fixed restore price, providing clear budget management.
- Avoids re-approaching the insurance market midterm as a distressed risk
- Remain on cover year round, even post loss.





Risk bursary

How will a risk bursary support you?



Policy onboarding

- Meet the S-RM Incident Response team & Recap policy information
- Incident hotline; Zero-dollar Retainer



Incident readiness

- Customised half day incident simulation



12-month ASM subscription

- Continuous attack surface monitoring
- In-depth vulnerability analysis



Targeted resilience assessments

- Data driven resilience assessments, offering clients valuable insights into their security posture and potential vulnerabilities

Our CyCore Asia Risk Enhancement Partnership

wtw



S-RM



Proprietary wording

“Coverage designed for Asia risks, by Asia-based experts”



We have developed **proprietary CyCore Asia wording** in collaboration with our in-house claims and legal experts. The outcome is a policy wording that is **broad, practical and easy-to-follow.**

Coverage benefits included as a standard in CyCore Asia wording (not exhaustive):

- System Failure coverage for your own Computer System or a Third-Party Service Provider’s Computer System
- Coverage for Claims Preparation Costs for Business Interruption claims
- Coverage for Business Interruption Events attributable to a Third-Party Service Provider – not limited to IT Providers

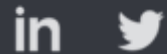
Thank You and Q&A

For more information

Visit our website at www.s-rminform.com

Email us at hello@s-rminform.com

CONNECT WITH US ON SOCIAL MEDIA



Important Information The information provided to you in this document is confidential and prepared for your sole use. It must not be copied (in whole or in part) or used for any purpose other than to evaluate its contents. No representation or warranty, express or implied, is or will be made and no responsibility or liability is or will be accepted by S-RM, or by any of its respective officers, employees or agents in relation to the accuracy or completeness of this document and any such liability is expressly disclaimed. In particular, but without limitation, no representation or warranty is given as to the reasonableness of suggestions as to future conduct contained in this document. Information herein is provided by S-RM Intelligence and Risk Consulting Ltd on our standard terms of business as disclosed to you or as otherwise made available on request. This information is provided to you in good faith to assist you in mitigating risks which could arise. No implied or express warranty against risk, changes in circumstances or other unforeseen events is or can be provided. S-RM Intelligence and Risk Consulting Ltd accepts no liability for any loss from relying on information contained in the report. S-RM Intelligence and Risk Consulting Ltd is not authorised to provide regulatory advice. S-RM Intelligence and Risk Consulting Ltd is registered in England with Number 05408866 with its registered office at: Beaufort House, 15 St Botolph Street, EC3A 7DT, United Kingdom.