Actuaries Institute.

Cyber Shadows:
Shaping scenarios to strengthening strategy

May 2026

Presented by Grace Ng and Devruchir Jain
Contributions by Augustine Sidik, Sinchana Gaddi and James Aclis

Presented at the 2026 All Actuaries Summit

The Actuaries Institute acknowledges the traditional custodians of the lands and waters where we live and work, travel, and trade.

We pay our respect to the members of those communities, Elders past and present, and recognise and celebrate their continuing custodianship and culture.

Setting the scene

THE CHALLENGE

- Cyber risk is one of the **most material yet least visible risks** facing organisations today.
- It develops **outside traditional risk signals** – embedded within technology complexity and across third-party dependencies.
- These cyber shadows can remain hidden until a disruptive events brings them to light.

THIS SESSION – TWO LENSES

LENS 01

Cyber Risk Scenarios for ICAAP Stress Testing

Assessing capital adequacy and insurer viability under severe but plausible cyber failure.

LENS 02

Cyber Risk Quantification for Management

Understanding, prioritising and actively managing cyber exposure in BAU decision making

Actuaries Institute.

ICAAP

Actuaries Institute.

Current landscape: Cyber risk scenarios in ICAAP

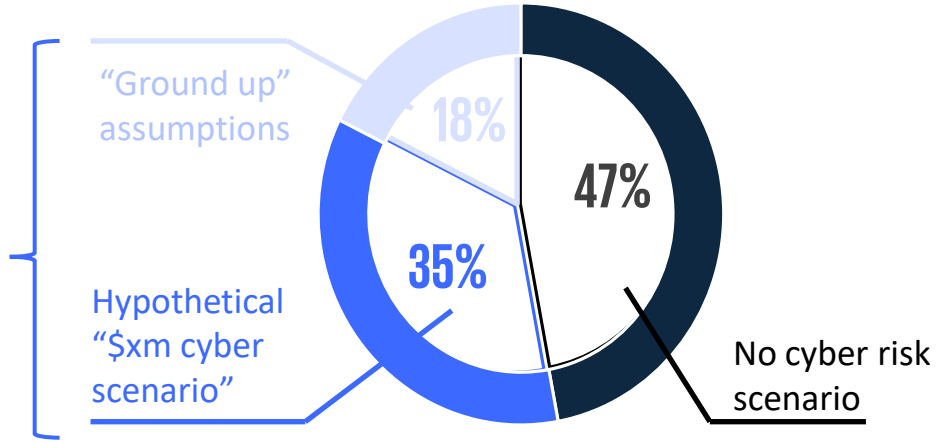
Current ICAAP stress testing framework

Strong emphasis on "well understood" risks

- Large amount of historical data
- Mature modelling techniques
- Clear traceability between assumptions and capital impact

93% Of GI and Health insurers identify cyber as a material risk

53% Include cyber scenarios in their ICAAP / Recovery Plan



Source: KPMG

A 40% gap between recognition and action – leaving capital adequacy assessments incomplete.

WHERE CURRENT ICAAP SCENARIOS FALL SHORT?

- Typically, only **one** cyber attack scenario is assessed.
- Scenario selection is based on perceived "most-likely" events, not structured threat analysis .
- Ground up assumptions are **high-level and lack empirical support.**
- Analysis focuses solely on capital impact – limited consideration of financial & operational effects.
- No frequency or probability assessment
- Resulting capital impact is generally immaterial.

Five key cost drivers of a cyber event (in addition to Ransom Payment)

Detection & Escalation 1

- Forensic investigation
- Incident response
- Initial legal advice in the first hours and days.

Typical cost nature:
Immediate; bounded

Post-Breach Response 2

- Customer notification
- Credit Monitoring
- Regulatory engagement
- Can reach **tens of millions** for large insurers, purely due to scale.
- Seldom the dominant source of solvency risk.

Typical cost nature:
Short-to-medium term; relatively bounded

Lost business & Reputation 3

- Business interruption
- Revenue leakage
- Customer attrition
- Long-term revenue erosion is difficult to attribute directly to a breach
- Often manifests through broker behaviour or renewal dynamics, rather than an immediate loss.

Typical cost nature:
Diffuse; Multi-year
Hard to attribute

Legal, Regulatory & Fraud 4

- Class actions
- APRA capital add-ons
- Multi-year litigation across parallel proceedings
- Dominates the **tail risk** of a cyber event

Typical cost nature:
Long tail;
Unbounded; capital critical

Security uplift 5

- System rebuilds
- Enhanced controls
- Third-party security assessments
- Pre-incident investment in security automation materially reduces breach costs: a forward-looking spend.

Typical cost nature:
Medium term;
Large but bounded

Actuaries Institute.

High-Level ranking the financial exposure

Indicative cost ranges, ranked by potential financial exposure.

Actual outcomes depend on the **nature**, **severity** and **duration** of the cyber event, and evolving **regulatory and litigation outcomes**.

Cost components may **crystallise concurrently or sequentially,** producing aggregate losses far exceeding any single component in isolation.

#	Cost Component	Cost duration	Indicative Range
Driver 4 – Legal, Regulatory & Fraud			
1	**Class action & litigation settlements** e.g. Medibank class action still unresolved. Scales with affected population × damages per person.	**Unbounded**	**$50M – $500M+**
Driver 4 – Legal, Regulatory & Fraud			
2	**Regulatory fines & APRA capital add-on** e.g. OAIC: up to $2.22M per contravention. APRA add-on: Medibank precedent of $250M.	**Unbounded**	**$20M – $300M+**
Driver 3 – Lost Business & Reputation			
3	**Long-term revenue attrition** Customer & broker churn, weaker growth, operational drag. Diffuse: hard to attribute to event	**2 – 5 years**	**$20M – $150M+**
Driver 5 – Security Uplift			
4	**Security uplift & remediation** Mandatory post-event spend. Medibank: $126M cumulative to date.	**1-3 years**	**$15M – $100M+**
Driver 2 – Post-Breach Response			
5	**Notification & credit monitoring** Predictable at scale: e.g. $15–30 per head + uptake rate for monitoring.	**3-12 months**	**$5M – $80M+**
Driver 1 – Detection & Escalation			
6	**IR, forensics & immediate legal** Retainer relationships and tested IR plans reduce this materially.	**Days - weeks**	**$2M – $15M+**

Actuaries Institute.

Has a cyber event ever caused an insurer to fail?

NOT YET

The hardest hit insurers - Medibank (AU, 2021), Anthem (US, 2015), CNA Financial (US, 2021) survived because they are **large, well-capitalised organisations.** Medibank's direct costs of AU$126M (to date) were manageable against ~AU$8B in revenue.

A small to mid-sized insurer with thin capital margins faces a materially different risk profile.

But it has **happened in other industries**. KNP Logistics Group – a 158 year-old British transport company – was forced into administration in 2023 after a ransomware attack devastated its operations, leaving 730 staff without jobs.

Large insurer
Top 5 by GWP (~60% of Industry GWP)

Starting PCA Multiple	Avg Capital ($m)	Loss to breach 1.3x	Loss to breach 1.0x
1.0 - 1.4			
1.4 - 1.6	914	225	500
1.6 - 1.8	3,340	1,518	2,520
1.8 - 2.0	3,200	1,543	2,503
> 2.0			

Medium insurer
Next 6 by GWP (~20% of Industry GWP)

Starting PCA Multiple	Avg Capital ($m)	Loss to breach 1.3x	Loss to breach 1.0x
1.0 - 1.4	743	45	206
1.4 - 1.6	601	41	170
1.6 - 1.8	623	76	202
1.8 - 2.0	838	195	343
> 2.0	507	221	287

Small insurer
All other insurers

Starting PCA Multiple	Avg Capital ($m)	Loss to breach 1.3x	Loss to breach 1.0x
1.0 - 1.4	205	-1	47
1.4 - 1.6	160	5	41
1.6 - 1.8	132	11	39
1.8 - 2.0	150	27	56
> 2.0	241	108	139

Source: APRA, KPMG, 31 Dec 2023

- **For an organisation of your size,** how would you *respond* to a cyber attack resulting in losses of this magnitude?
- **Given your current PCA multiple**, have you considered *stress-testing* cyber scenarios of this scale?
- To what extent does your **cyber insurance** cover this exposure?

Actuaries Institute.

Is Cyber Risk an IT/Operational Problem or a Balance Sheet Risk?

Common perceptions	What the evidence shows	The landscape is shifting
"Cyber is an IT/CISO responsibility"	Litigation tail can **exceed $500m** for large insurers	**Regulatory mandate:** APRA requires boards to stress-test material operational risks, and **cyber is increasingly material.**
"We have cyber insurance – we're covered"	Cyber policies contain **exclusions that may not respond**	
"Our operational risk charge captures it"	Standard OpRisk charge doesn't capture tail risk or differentiate between strong and weak controls	**Real losses at scale:** Medibank (2021) (AU$126M+), CNA Financial (2021) ($40M ransom), Anthem (2015) ($260M) are anchors, not hypotheticals
"It hasn't happened to us before"	Medibank precedent: direct cost $126m, APRA $250m add-on, class action unresolved	
"A breach would cost a few million at most"	APRA can impose **capital add-ons post event** when controls are weak.	**The threat is evolving:** AI-accelerated attacks compress dwell times from weeks to hours. The next event may look nothing like the last.
"We've done an ICAAP stress test and it's unlikely to have a material capital impact"	Cyber attack has caused companies in other industries to **collapse** (e.g. the KNP Logistics Group in the UK in 2023)	

Actuaries Institute.

From Cyber Threat to Capital Adequacy:

An Integrated Prudential Narrative

CPS 234

Information Security

"The What"

- Defines the **technical nature of cyber risk**
- Requires insurers to identify their crown-jewel information assets, assess vulnerabilities, and test security controls against credible threat scenarios.
- It provides the **realistic cyber events,** such as ransomware or data exfiltration, that form the **basis of stress testing.**

Output: **realistic cyber events** – not yet quantified financially

CPS 230

Operational Risk Management

"The So What"

- Translates threats into **operational consequences –** service disruption, third-party failures, recovery costs.
- Requires insurers to stress test severe disruptions, to determine whether critical services can be maintained within tolerance.

Output: **where losses arise** – interruption, degraded delivery, remediation

CPS 220

Risk Management

"The Governance Bridge"

- Embeds cyber in the enterprise risk framework.
- Ensures Board ownership and alignment with Risk Appetite.
- Provides governance over how operational disruptions inform risk, resilience, and capital decisions.

Output: cyber risk is **assessed in the context of strategy and risk appetite.**

GPS / LPS 110

Capital Adequacy

"The How Much"

- Through ICAAP cyber stresses are quantified in $ terms and tested against available capital.
- Adequacy is assessed under scenarios where controls fail and recovery is constrained.

Output: **capital held is adequate**, or a gap is identified requiring action.

Actuaries Institute.

ICAAP scenarios, anchored in real events

SCENARIO 01

Ransomware & Operational Disruption

Own systems encrypted. Core operations offline 4–6 weeks.

- Business interruption (lost premium, claims delays)
- Ransom decision — pay or rebuild
- Security uplift & IR costs
- APRA capital add-on risk for control gaps

Anchor: CNA Financial 2021 ($40M ransom)

SCENARIO 02

Large-Scale Data Exfiltration

Millions of policyholder records stolen and published.

- Notification & credit monitoring at scale
- OAIC civil penalty proceedings
- Class action — largest potential cost
- Multi-year litigation defence

Anchor: Medibank 2022, Anthem 2015

SCENARIO 03

Third-Party /Supply Chain Event

Critical vendor breached — insurer still holds liability.

- Regulatory obligation regardless of source
- Indemnity dispute with vendor
- Claims TPA or cloud provider failure
- Operational disruption from dependency
- Reputational damage

Anchor: MOVEit 2023, Medibank entry vector

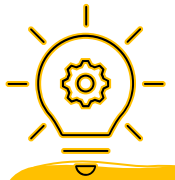
SCENARIO 04

Systemic / Industry-Wide Event

Shared infrastructure exploited across multiple insurers.

- Correlated losses across the industry simultaneously
- Common cloud provider
- Reinsurance and cyber insurance market stress

Anchor: CrowdStrike outage 2024 (non-malicious), AWS outage (late 2025)



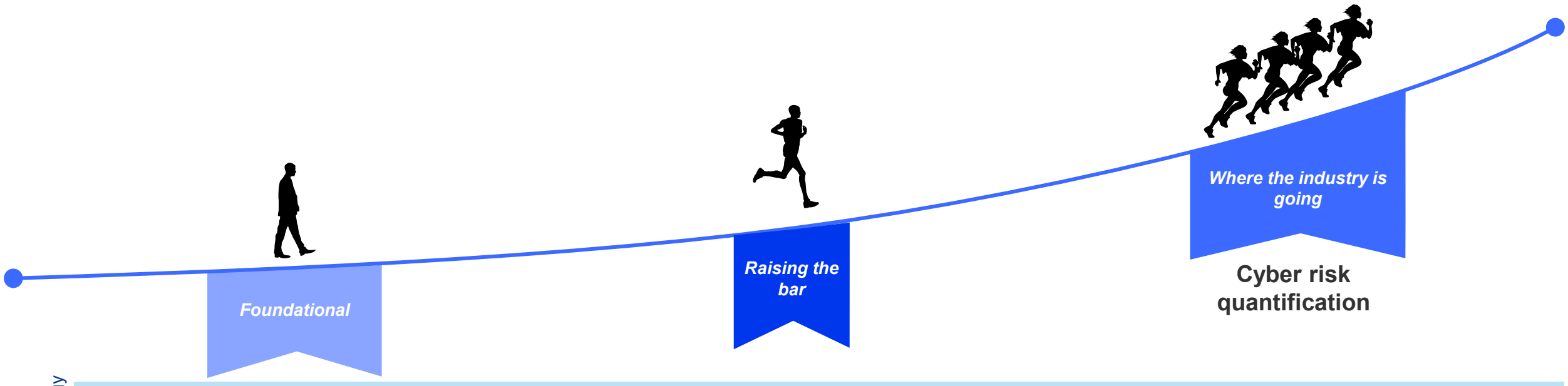
What do you think are the potential scenarios worth considering for your organisation?

Actuaries Institute.

Cyber risk quantification

Actuaries
Institute.

Cyber Risk Management Journey



	Foundational	Raising the bar	Where the industry is going
Reporting methodology	**CSF-based (NIST, E8, CMMI etc)** Industry standard used for maturity-based assessment of cyber capabilities.	**Qualitative risk scenarios** Cyber capability is expressed as a function of key business risks.	**Quantitative risk scenarios** Cyber capability and the resulting dollar value impact of key business risks are reported to executives.
Reporting Capabilities	• Point-in-time report on cyber maturity • No direct way to have a risk buy-down focus • Maturity is based on an industry-standard	• Scenarios based on key business risks • Cyber capability reported on a risk matrix, aligning with how other risks are reported on • Reporting focuses on capabilities that map to the organisation's key risks	• Cyber risks are reported with expected loss dollar values • Top capabilities to buy-down cyber risk are identified • Real-world threat landscape is incorporated

Actuaries Institute.

Contextualising cyber exposures

Attack paths consist of 5 steps, each representing techniques a threat actor might use and the defenses needed to stop them. Some steps may not apply in all cases, such as insider breaches where initial compromise isn't relevant.

05 **Scenario Likelihood**

Output from the model: the likelihood of the scenario occurring.

04 **Attack Path Step**

The attack path steps that lead to the cyber risk scenario occurring.

03 **Techniques**

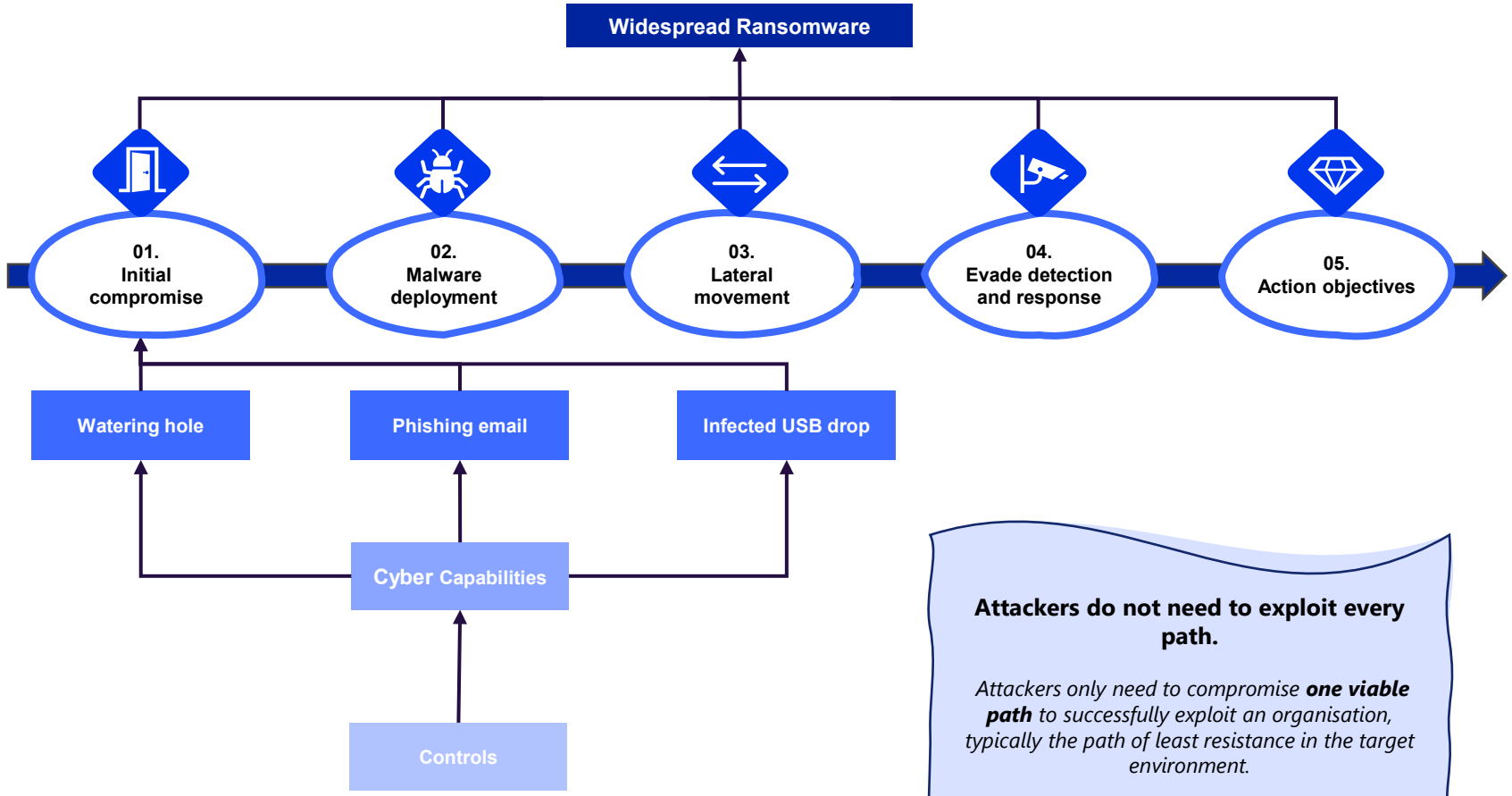
The different ways an attacker can breach each attack path step.

02 **Cyber Capabilities**

The capabilities in the cyber model that defend against the techniques attackers use.

01 **Controls**

Client control frameworks can be mapped to cyber capabilities to inform scoring.



Attackers do not need to exploit every path.

*Attackers only need to compromise **one viable path** to successfully exploit an organisation, typically the path of least resistance in the target environment.*

Actuaries Institute.

Preparing for the journey

Scenario Selection

Scenarios: In-scope scenarios are selected with the client, to identify which cyber risks are relevant, considering multiple factors.

- **Prioritise**: Time and capacity limitations will restrict what can be assessed.
- **Threat landscape**: Evaluate trends seen in the marketplace (e.g. a rise in DDoS attacks, uptick in ransomware).
- **Industry sector**: Consider peers and what threats are faced by comparable organisations.
- **Client specific factors**: Previous incidents observed, board concerns, or regulatory requirements (e.g. FCA 166 notices).

Capabilities Assessment

The **effectiveness** of capabilities is **determined** by measuring **three metrics** that are **multiplied together** to produce the overall score:

Likelihood reducing

X

Impact reducing

X

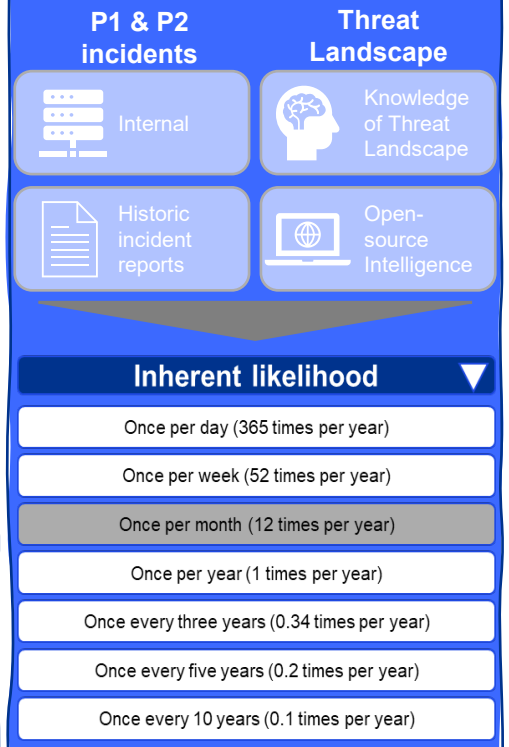
Foundational

=

Capability Effectiveness

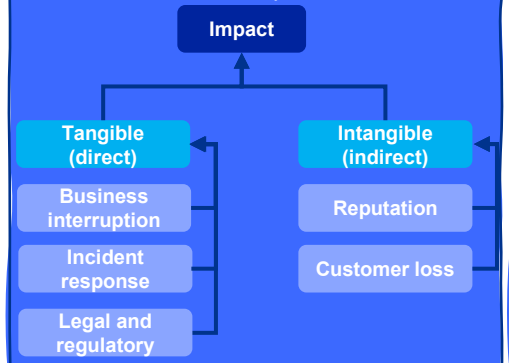
Attacker Contact Rate (ACR)

Inherent likelihood: A quick way to determine ACR is to review threat intelligence and determine a total value. This is referred to as inherent likelihood.



Impact Estimate

Decomposition: Impact is measured by breaking the loss down into the different types of impact that are caused. A calibrated estimate is then produced for each impact.



Cyber loss: The impact caused to the organisation by a cyber risk scenario. This is can be expressed financially or operationally.

Initiatives

Use outputs to inform initiatives:

IDENTIFY

Cyber risk quantification helps our clients identify and **quantify cyber risks** in financial terms

PRIORITISE

It enables our clients **to prioritise investments** in cyber controls for maximum **risk reduction**.

REPORT

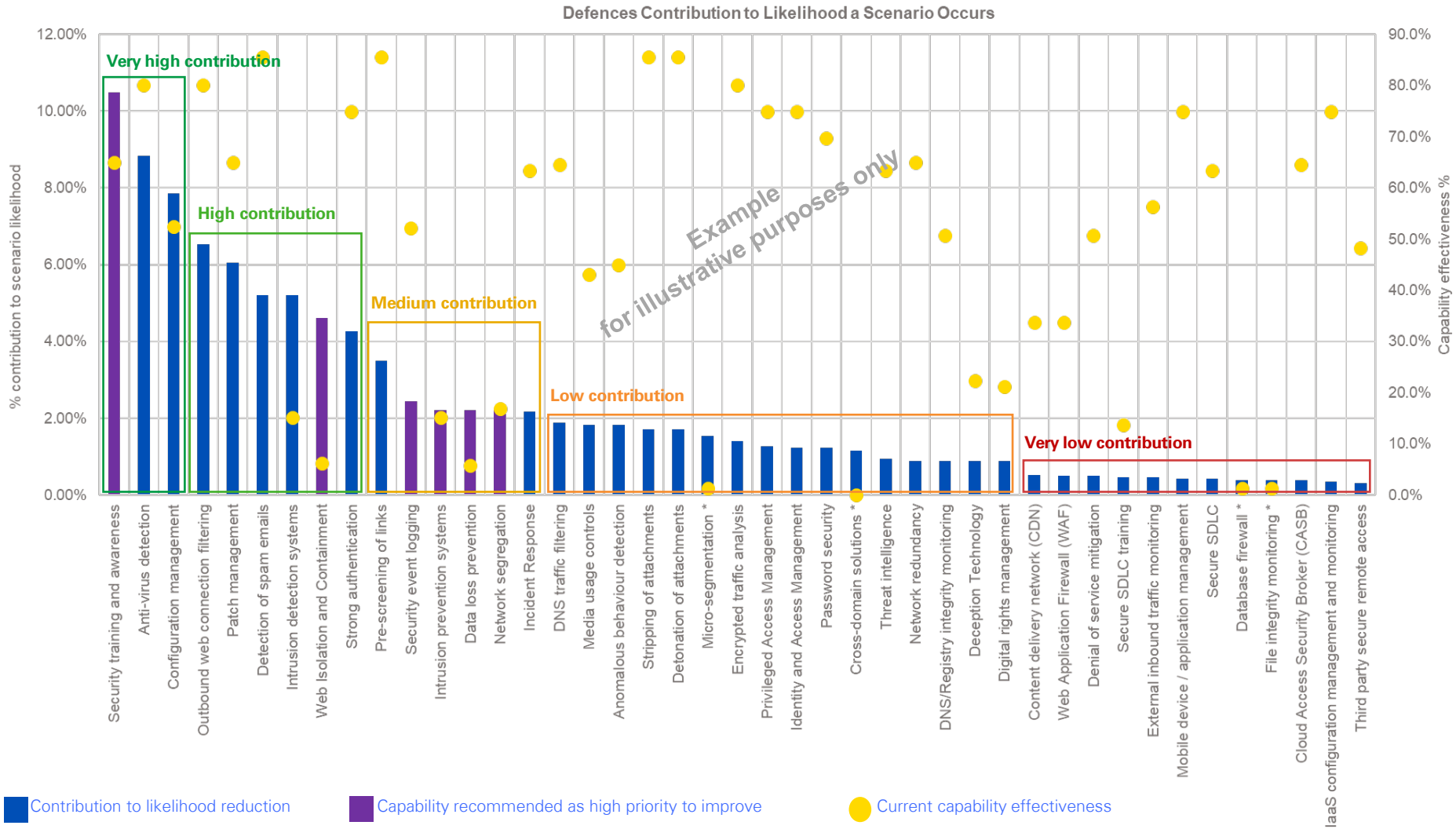
Cyber risk quantification enhances **board-level reporting** with quantitative measures, making it easier to communicate and get buy-in from stakeholders.

BENCHMARK

Cyber risk quantification allows our clients to **benchmark** their cybersecurity posture against industry peers.

Actuaries Institute.

Visualising outputs – Control prioritisation



Key Cyber Risk Quantifications

1 Capabilities with **Low Capability Effectiveness** and **High or Medium Contribution** should be prioritised for further improvement. In this example, this included:

- Network segregation
- Security training & awareness
- Data loss prevention
- Web isolation and containment
- Network visibility (security event logging)
- Intrusion detection systems

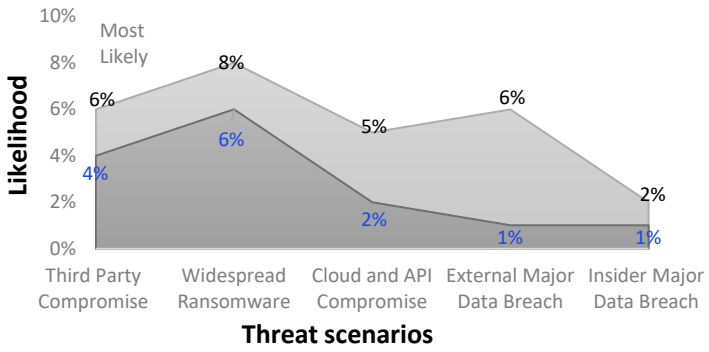
2 Top 10 capabilities contributed to ~63% of total likelihood reduction based on current cyber capability effectiveness estimates.

3 Long thin tail showing that many cyber capabilities have limited / very low effect on cyber risk scenario likelihood reduction.

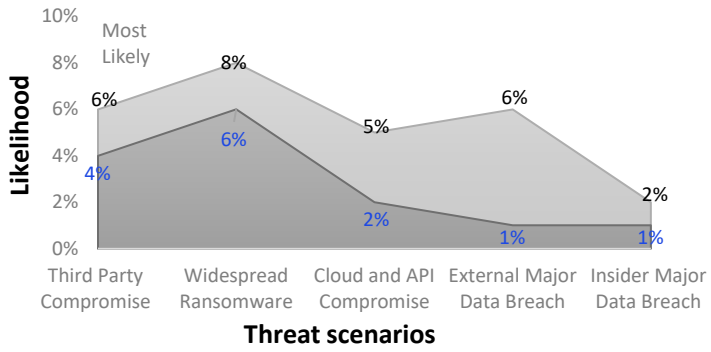
Cyber Exposure

Top cyber threats in large FS organisations

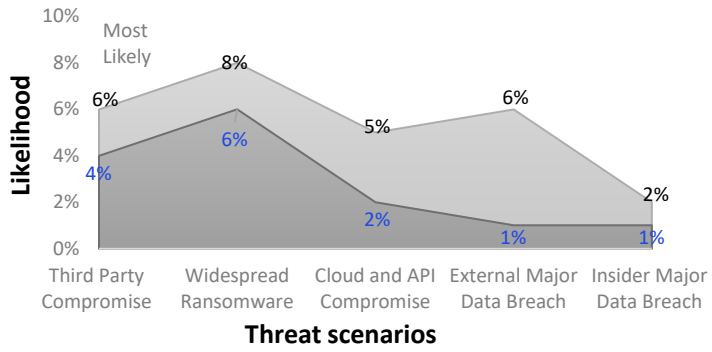
Large (More than $1Billion)



Medium ($100 million - $1Billion)



Small (Up to $100 million)



Indicative losses large in FS organisations

Large (More than $1Billion)

Scenario	Most likely to worst losses
Insider major data breach	$31M to $155M+
External major data breach	$16M to $155M+
Third-party compromise	$23M to $155M+
Widespread ransomware	$47M to $310M+
Cloud environment compromise	$35M to $233M+

Medium ($100 million - $1Billion)

Scenario	Most likely to worst losses
Insider major data breach	$16M to $78M+
External major data breach	$8M to $78M+
Third-party compromise	$13M to $93M+
Widespread ransomware	$27M to $155M+
Cloud environment compromise	$22M to $124M+

Small (Up to $100 million)

Scenario	Most likely to worst losses
Insider major data breach	$6M to $39M+
External major data breach	$3M to $31M+
Third-party compromise	$5M to $47M+
Widespread ransomware	$16M to $93M+
Cloud environment compromise	$13M to $62M+

Closing Thoughts

Looking ahead

The cyber threat landscape is become faster-moving, more scalable and strategically complex. The question is no longer *whether* cyber events will occur - but whether we are **learning enough from events today to shape stronger outcomes tomorrow**.

- **ICAAP stress testing asks *"Can we survive?"***
- **Management quantification asks *"How do we become stronger?"***

Together, they turn cyber shadows into **clarity, confidence, and action**.

Food for Thought

- Is your organisation treating cyber primarily as a risk to be actively managed?
- Is cyber risk being managed on a forward-looking basis, or largely addressed after control failures, incidents, or near misses?
- Do you have clear visibility over legacy systems, deferred patching, control exceptions, and temporary workarounds that elevate cyber risk?
- Is cyber risk management aligned with the organisation's third-party and outsourcing strategy?
- Is cyber insurance being used to support resilience and recovery, or implicitly to justify accepting higher operational or technology risk?
- Is awareness of cyber policy wording, exclusions, sub-limits, and conditions embedded in management decision-making?

Actuaries Institute.

Actuaries Institute.

Thank you

Actuaries Institute
actuaries.asn.au