

Cyber Security Threat Landscape

Pat Larkin pat.larkin@ek.co

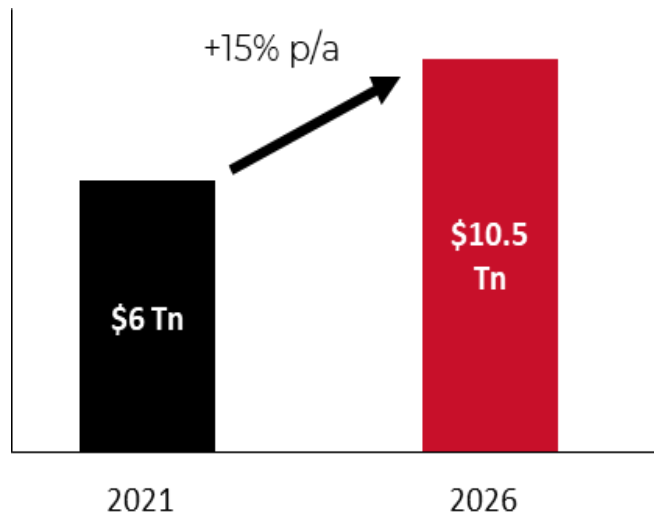


Objectives

- Overview of the Cyber Threat environment
- Outline current major Cyber Security threats
- Outline what a resilient organisation looks like
- Deeper dive on AI risk

Cybercrime as an economy

Global cost of Cybercrime



Source: Cybersecurity Ventures

Top 3 Economies Globally

1



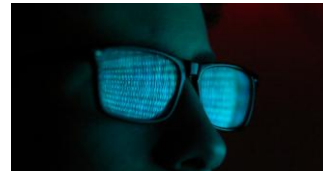
USA

2



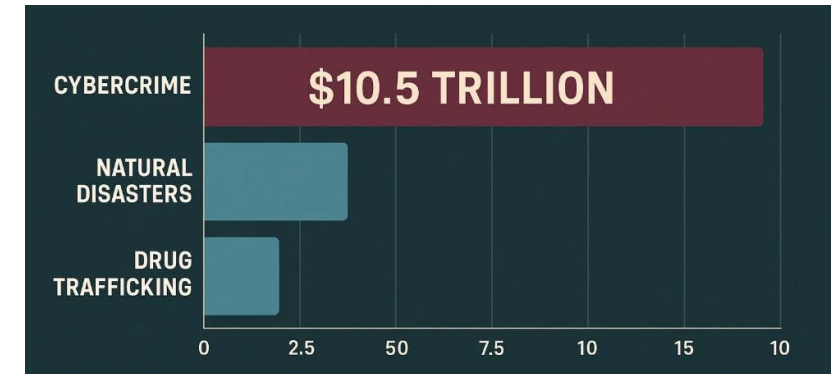
China

3



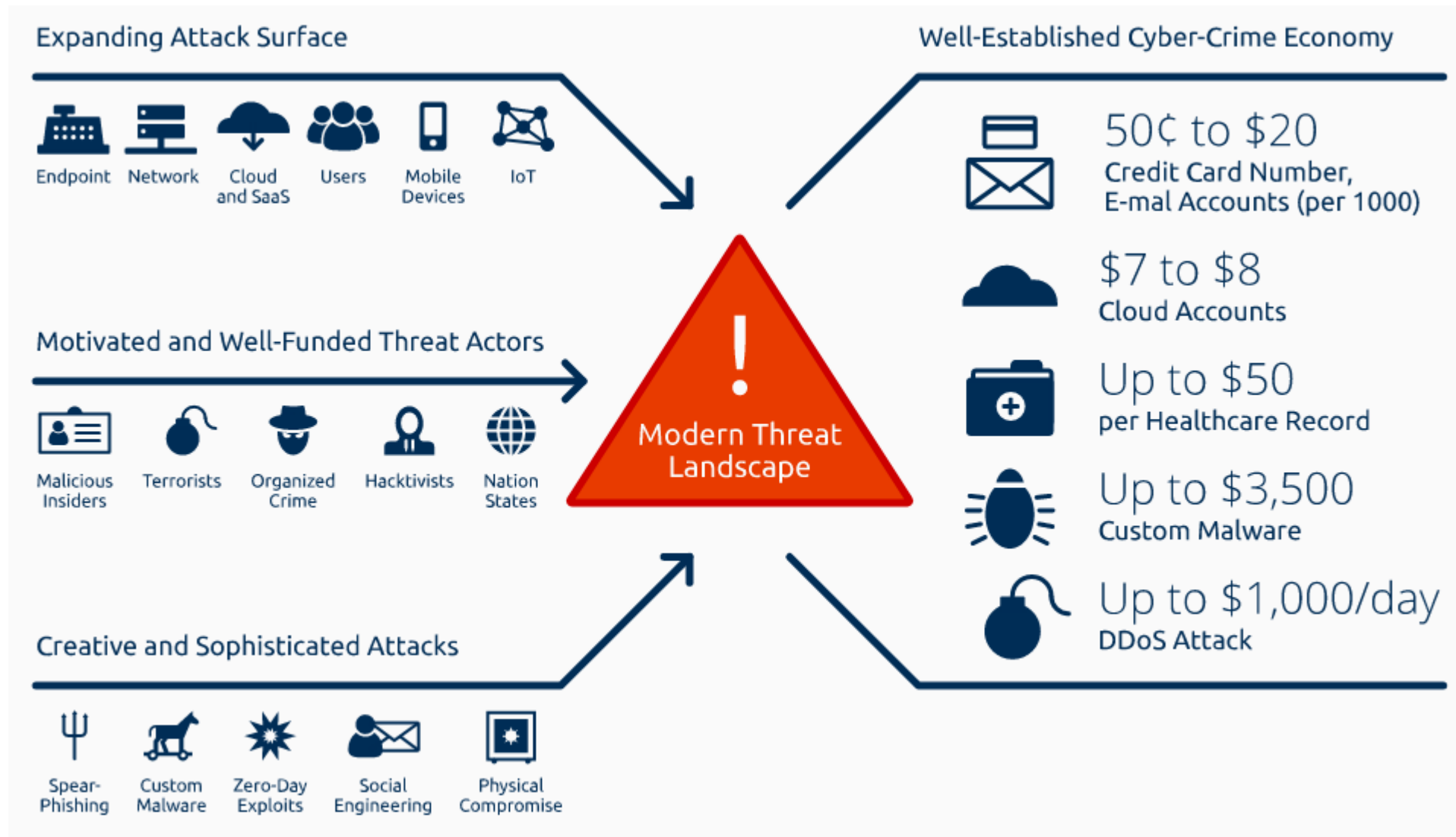
Cybercrime

Top of the big ticket costs



Probably one of the greatest wealth transfers in history?

Relentless cybercrime growth will continue



2026 Threat Landscape



2026 Top security threats



Ransomware & Data Extortion

Attackers now exfiltrate data before encryption, creating dual leverage - operational disruption and regulatory exposure. Financial institutions face reputational damage even when backups exist.

Identity Compromise

Credentials remain the primary entry vector. Attackers bypass perimeter defences by simply logging in using stolen or compromised identities, exploiting trust mechanisms.

AI-Enabled Social Engineering

Artificial intelligence accelerates reconnaissance, enhances social engineering, and automates attack workflows. Threat actors operate at unprecedented speed and scale.

Attack Surface Sprawl

Cloud sprawl, forgotten assets, and unpatched systems expand the attack surface. Most breaches exploit known vulnerabilities that organisations failed to remediate.

3rd Party & Supply Chain Exposure

Dependencies on vendors, cloud providers, and managed service partners create indirect risk. A compromise at a trusted third party can cascade across multiple institutions.

Insider Threats

Data-loss risks from trusted users who intentionally steal data or accidentally expose it. Because they have legitimate access, sensitive information can be copied or shared before controls detect it.

Three Blind Spots

All three exploit one common weakness: trust without verification

04

Attack Surface Sprawl



Cloud assets multiply faster than security teams can inventory them. Forgotten S3 buckets, unpatched VMs, shadow AI and legacy SaaS apps remain exposed for months.

Most breaches

Exploit known vulnerabilities that were never patched

05

Third-Party & Supply Chain



Vendors, SaaS providers, and managed service partners hold privileged access to your environment. A compromise at any one of them cascades through their customer base.

One vendor

Breach can touch hundreds of institutions simultaneously

06

Insider Threats



Employees, contractors, and departing staff hold legitimate access. Whether malicious or accidental, data leaves through sanctioned channels & bypasses perimeter controls entirely.

Hardest to detect

Because every action looks like normal business

The organisational attack surface

External, internal, physical and AI exposure, managed as one continuous lifecycle



External attack surface

Internet-facing and third-party exposure

- Domains, subdomains, DNS & IP ranges
- Websites, APIs & remote access (VPN/RDP)
- Cloud, SaaS & exposed storage buckets
- Shadow IT & forgotten legacy assets
- Third parties, leaked credentials, phishing



Internal attack surface

What an attacker reaches once inside

- Endpoints, servers, IoT & OT devices
- Identities: privileged & service accounts
- Flat networks & lateral movement paths
- Unpatched software & weak configurations
- Insider threat & sensitive data stores



Physical attack surface

Sites, hardware and people on the ground

- Offices, data centres & server rooms
- Badge access, tailgating & unattended areas
- USB ports, rogue devices & implants
- Lost or stolen laptops and phones
- Home offices, CCTV & building systems



AI attack surface

Cuts across all three surfaces

Prompt injection

Jailbreaks and manipulated LLM apps and chatbots

Model & data theft

Poisoned training data, stolen or tampered models

Agents & plugins

Excessive permissions and insecure tool access

Shadow AI

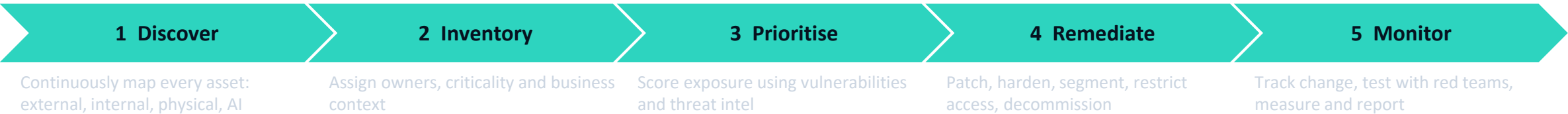
Sensitive data pasted into public GenAI tools

AI-powered attacks

Deepfakes, tailored phishing, automated recon

Attack surface management lifecycle

 Continuous loop back to Discover



What a cyber-resilient organisation looks like

Six capabilities working together around a resilient core



Hallmarks of resilience

- Leadership buy-in**
Security is a business priority, not an IT afterthought
- Culture, not compliance**
Every employee treats security as part of their job
Assume a breach mindset
- Continuous testing**
Regular red-teaming, tabletop drills and audits
Executive and board TTX's
- Third-party assurance**
Vendors and the supply chain held to the same bar
Assure and be ready to be assured

THE AI JOURNEY



3. Business Risks:

Compliance gaps, misinformation, security threats & loss of control



2. Unleashing Benefits:

Boosted productivity, automation & innovation



1. AI Explosion:

The rise of tools like ChatGPT & Copilot – transforming how we work



4. Defend & Protect:

Adapting security strategies to safeguard against AI-powered risks



5. Strategic AI Advantage:

Leveraging AI to outpace threats & gain a competitive edge



What is Artificial Intelligence?

Artificial Intelligence (AI)



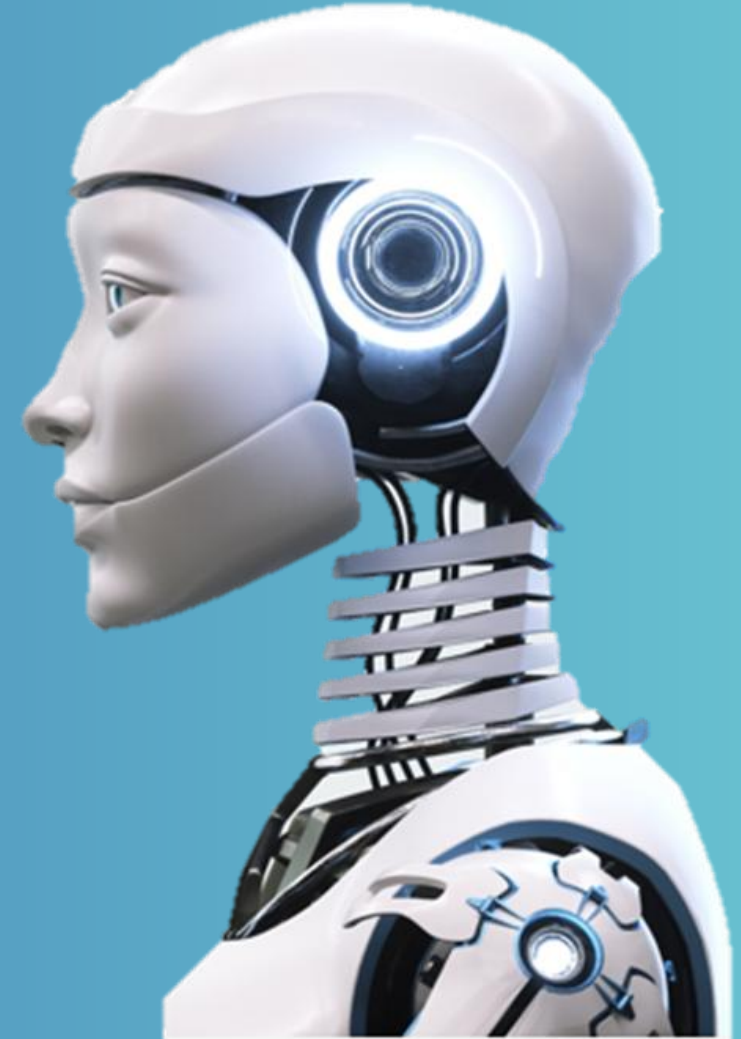
Simulates human intelligence in machines.



Includes machine learning, natural language processing & robotics.



Used in Healthcare, Finance, Automotive and more.



Attributes	GenAI	Agentic AI
 Definition	AI systems that generate content (text, code, images, etc.) based on prompts	AI systems that plan, reason, and act across multiple steps to achieve a defined goal
 Core Behavior	Predicts the next output based on input (e.g., next word, token, or pixel)	Takes initiative, capable of decision making, executes actions, and can operate independently
 Use Cases	Code generation, content creation, summarization, education, chatbots, image/video creation	Customer support automation, IT operations, multi-step strategies, security, and fraud detection
 Examples	ChatGPT, Claude, GitHub Copilot	ChatGPT agent, Cursor agent mode, Manus

Three Classes of AI Risk

A simple framework for organising AI risk conversations: the risk of AI itself, risk from AI-enabled attacks, and risk to your own AI systems.



Risks of AI

Broader societal & ethical impact

- Job displacement & workforce disruption
- Wider societal disruption
- Environmental impact
- Ethics, bias & loss of autonomy
- Privacy erosion & IP infringement



Risks from AI

AI used to attack the organisation

- AI-crafted phishing & deepfakes
- Automated social engineering
- AI-accelerated vulnerability discovery
- Disinformation campaigns
- Malicious content generated at scale

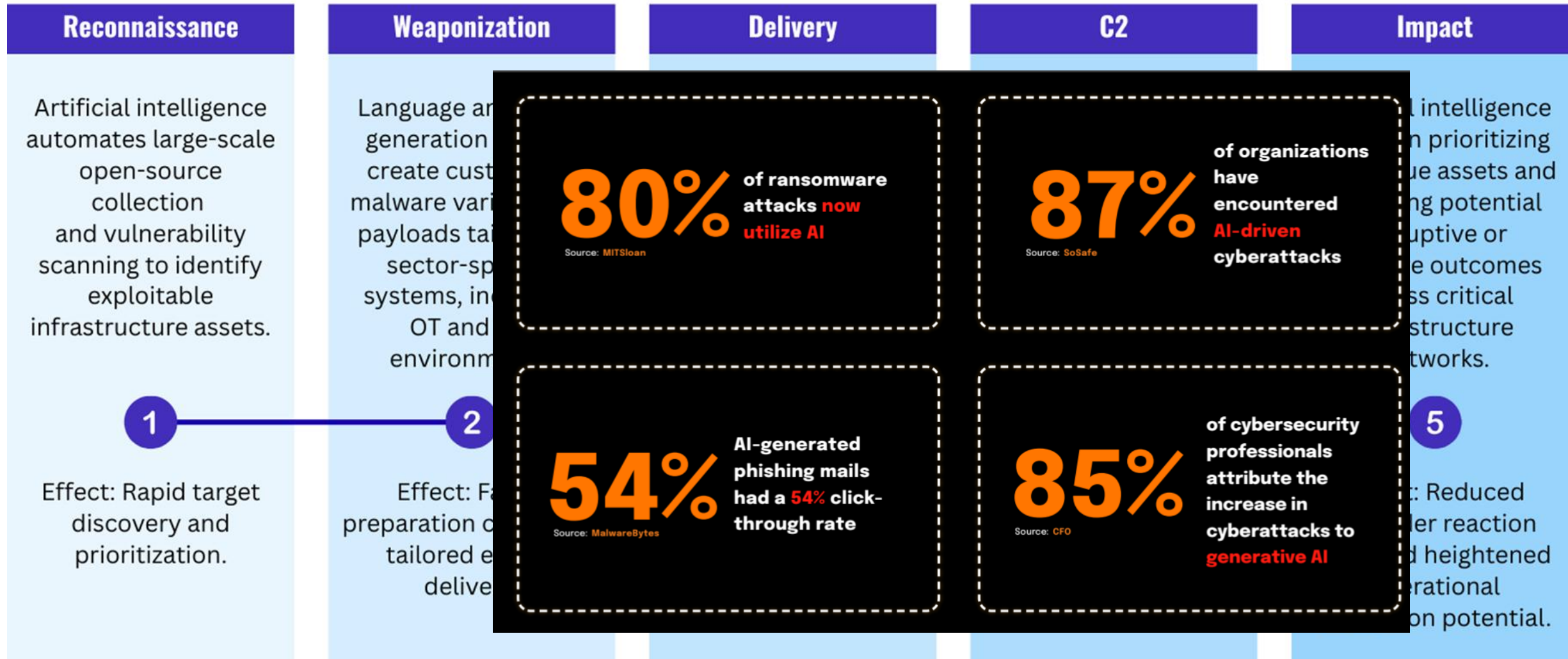


Risks to AI

Own AI services & infrastructure

- Model & training-data theft
- Data / model poisoning
- Prompt injection & jailbreaks
- Adversarial inputs & evasion
- Availability / denial-of-service

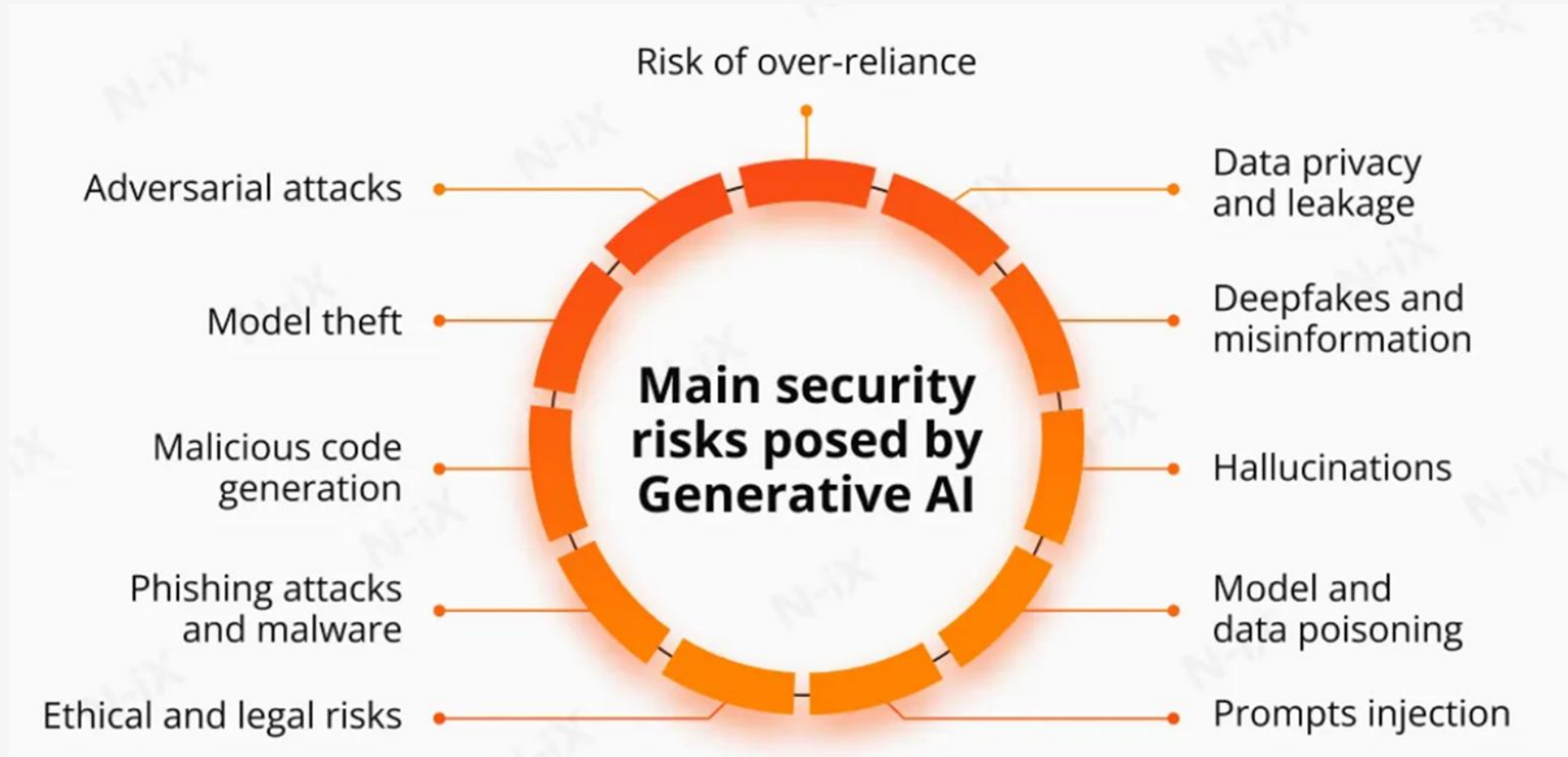
AI augmented attack flow



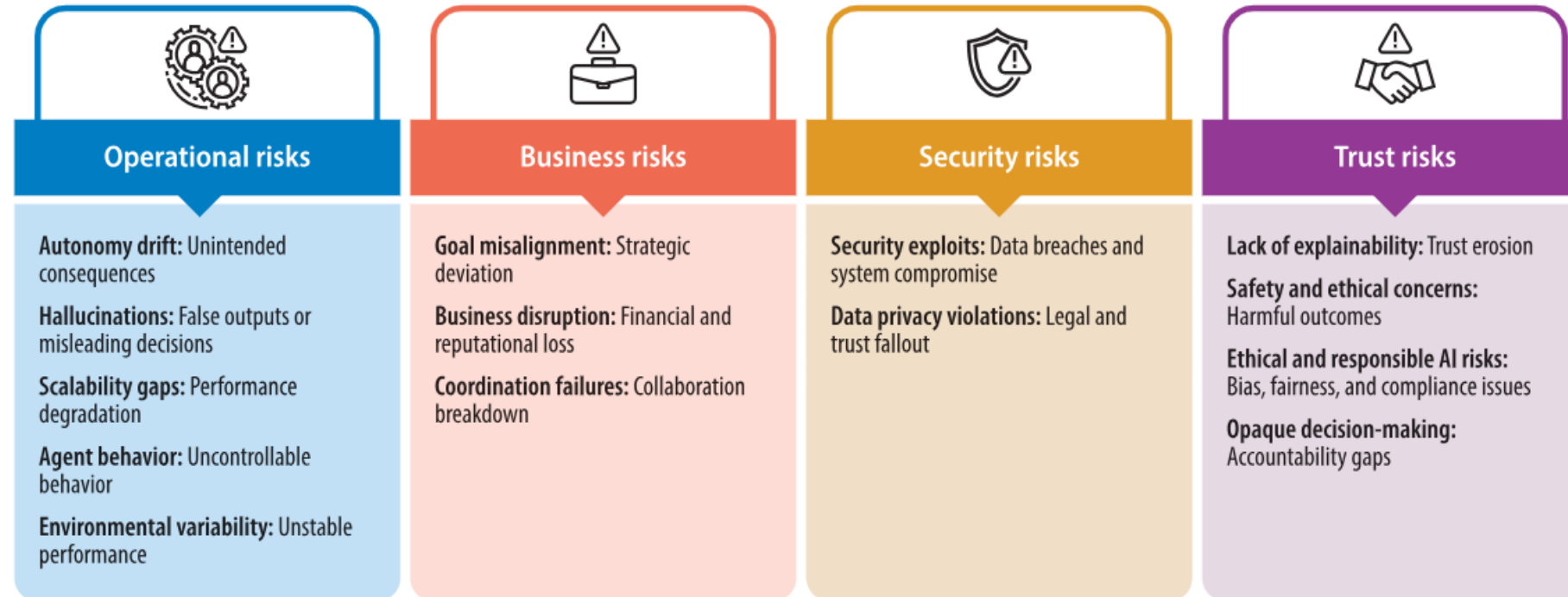
AI Levels the Pitch for the Defence Side



Generative AI Risks

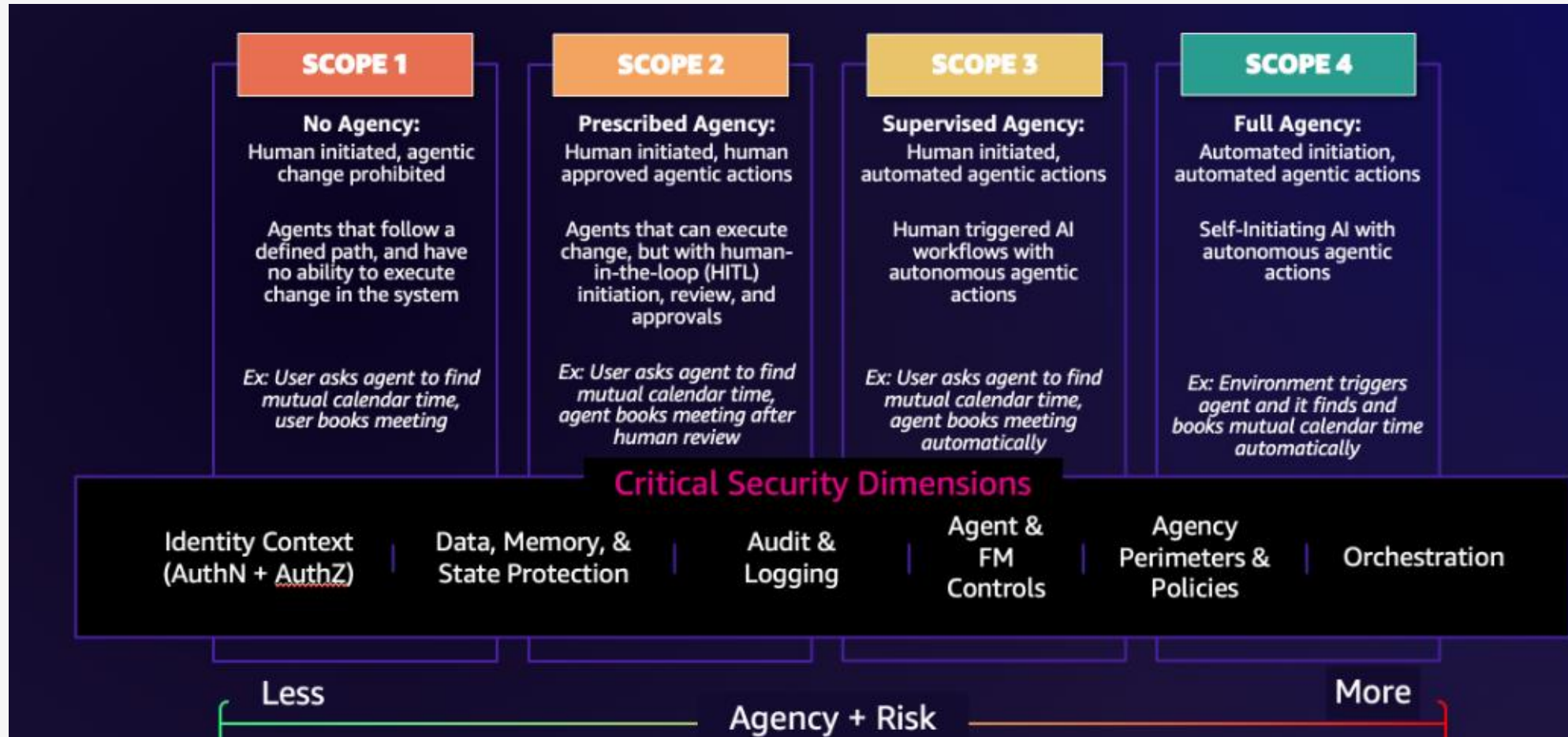


Agentic AI Risks



The AI Data Trust Paradox 76% of Data Leaders state employee trust AI Data powering their AI systems and are letting agents use this data, but data leaders don't have confidence in the data and the employees' data literacy

Agentic AI Autonomy Matrix



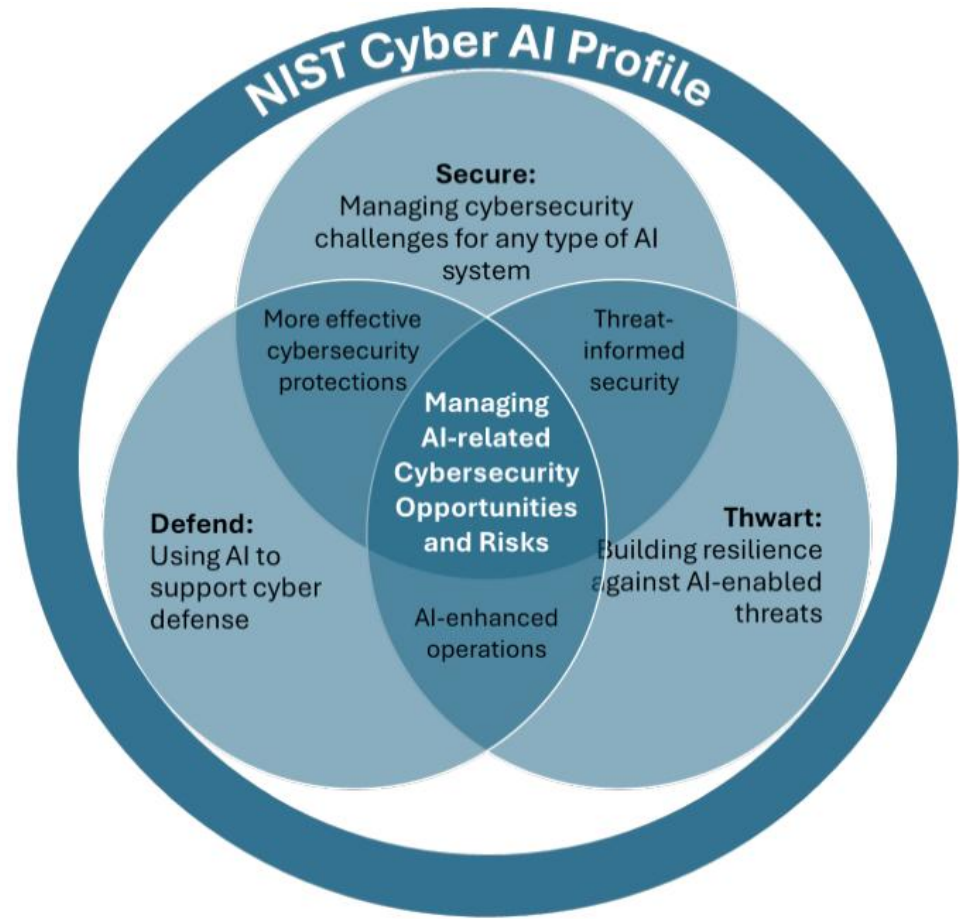
AI Risk Management

AI Standards and Frameworks

- ✓ EU AI Act
- ✓ ISO 42001
- ✓ NIST AI RMF
- ✓ NCSC Guidance

Core AI Security Components

- ✓ Governance
- ✓ Data Integrity & Privacy
- ✓ Transparency & Explainability
- ✓ Human Oversight
- ✓ Ethics
- ✓ Robustness & Reliability
- ✓ Controls & enforcement



Controls and enforcement.



SEE IT

AI Detect

Find every AI tool in use, rank the risk, prioritise action.

STANDARD



STOP IT

AI Shield

Block risky AI, enforce policy, protect data automatically.

STANDARD



TRAIN IT

AI Aware

Make every employee a safe, confident AI user.

STANDARD



GOVERN IT

AI Compliance

Data governance that prevents customer & company data leakage.

STANDARD



USE IT

AI Learn

Practical Copilot training that turns adoption into output.

PREMIUM – COMING SOON

OUTCOME AI enablement + AI security + AI governance, delivered together.



The impact of incident on organisations

Impact of Cyber Incidents on Organisations



Financial

\$4.44M avg breach cost
\$10.5T global cybercrime



Share Price

Okta lost \$2BN valuation
JLR stock price drop 5%, \$2BN
M&S share price slid 14.3%



Operational

23-day avg downtime
45% supply chain attack risk



Staff

Burnout, 38% attrition post-incident



Regulatory

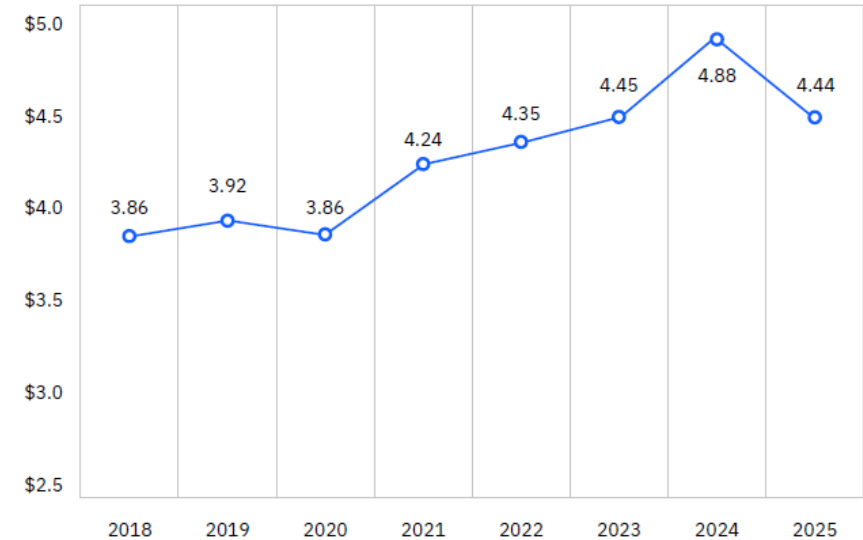
GDPR, NIS2, DORA fines and legal actions



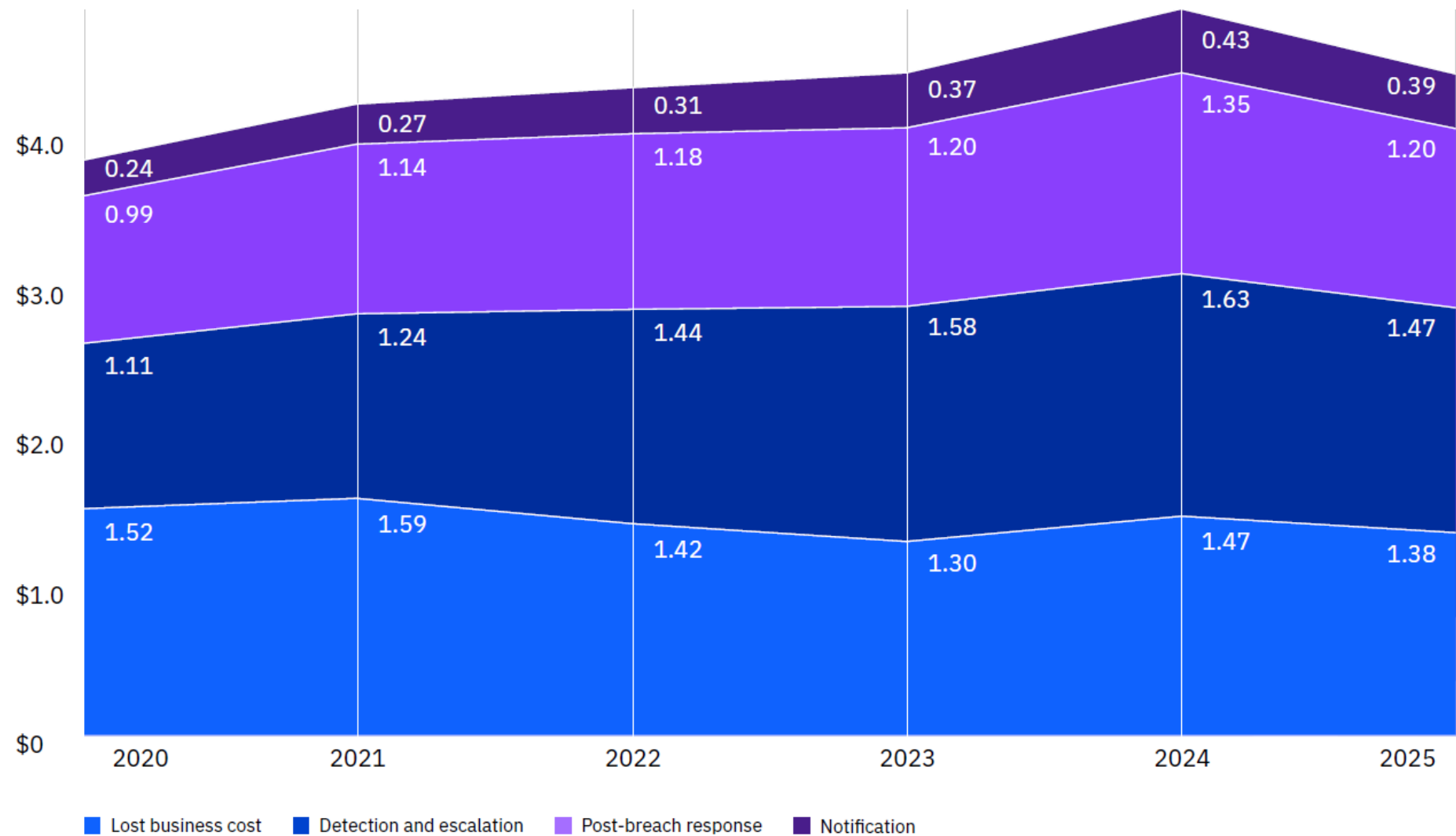
Insurance

Cyber insurance premiums up 28%,
levels of cover dropping, exclusions
widening

Figure 1.
Measured in USD millions



Avg \$4.44M data breach cost breakdown



Ponemon Cost of a Data Breach report 2025

Recovery Time

- Low Recovery Rates

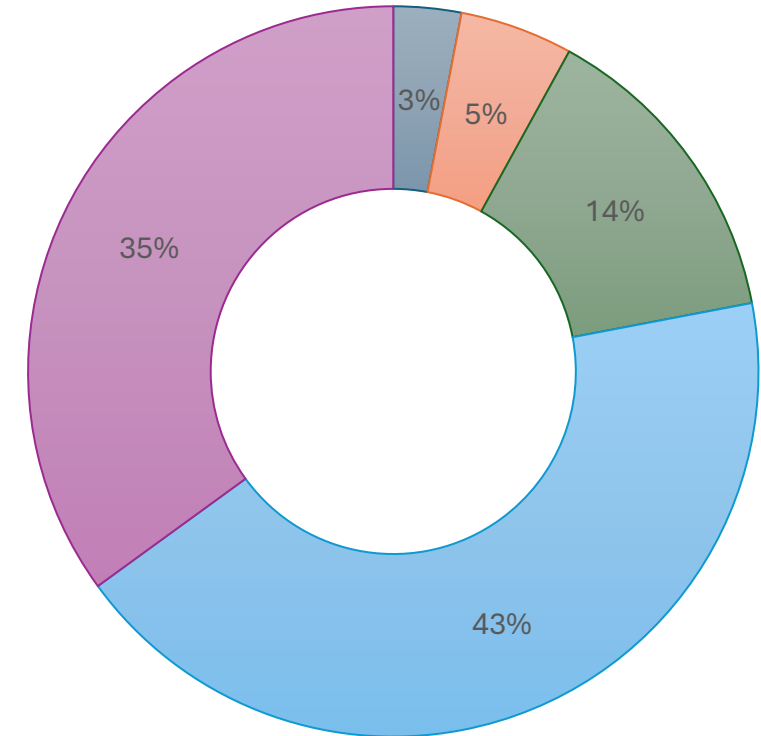
- Only 12% of organizations fully recovered from data breaches when questioned
- Most organizations are still working on recovery

- Recovery Timeframes

- More than 100 days for full recovery for over three-quarters of organizations
- Roughly one-third required more than 150 days
- 3% recovered in less than 50 days

Average Time to Recover

■ <50 Days ■ 51 to 75 ■ 76 to 100 ■ 101 to 150 ■ > 150



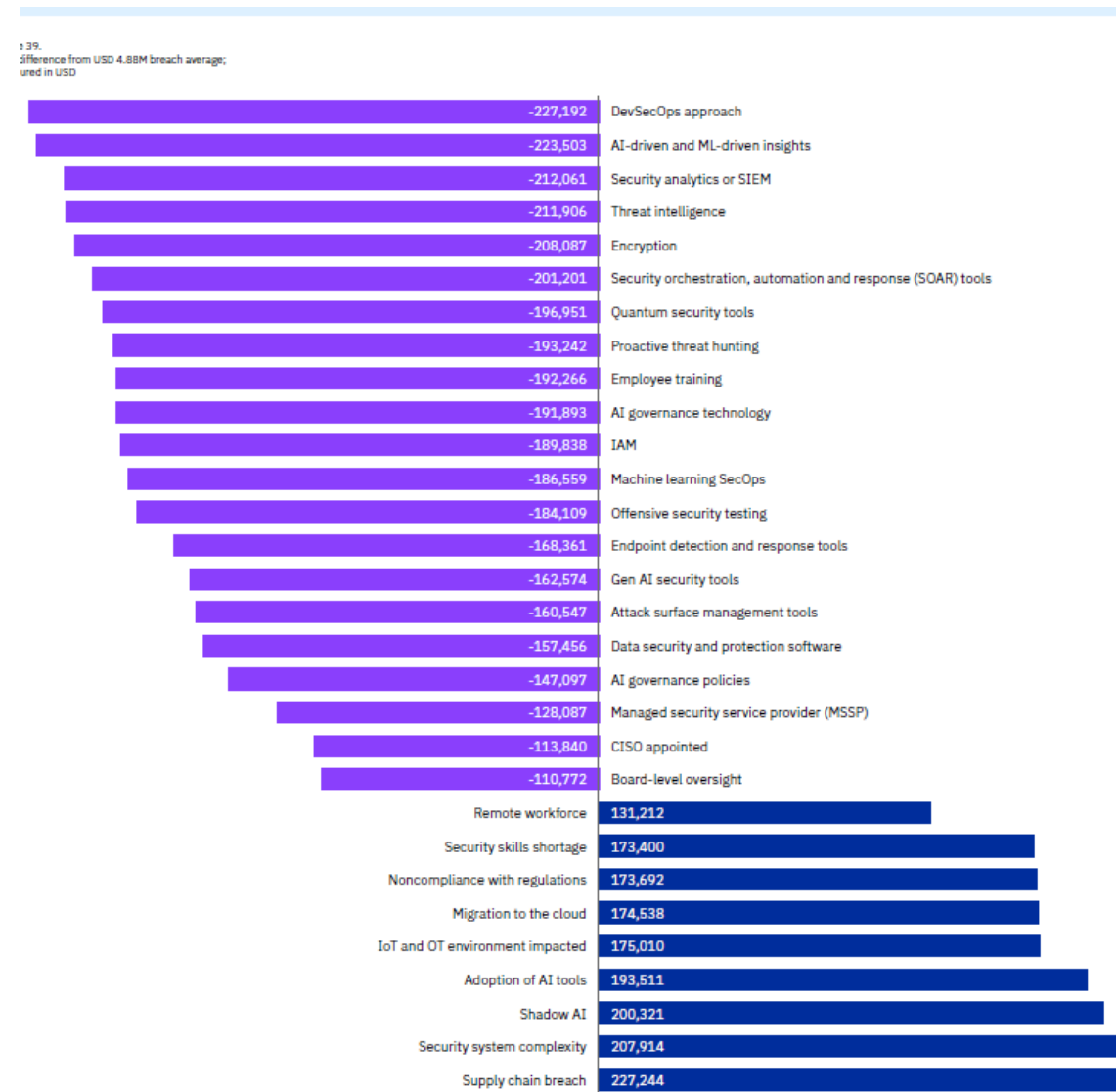
Factors Affecting Breach Costs

Factors that decreased costs

- Employee training
- AI and machine learning insights

Factors that increased costs

- Security system complexity
- Security skills shortage
- Third-party breaches



Systemic Governance, Risk & Compliance pays

Cyber Maturity Levels					
NIST CSF 2.0					
	L1 Initial	L2 Risk Assessed	L3 Repeatable	L4 Adaptable	
	Features	Risk Mgmt. measures are ad hoc, reactive, informal	Risk identified. measures implemented systemic	Risk Identified measures implemented systemically	Proactive, Risk Mgmt fully integrated, continuous improvement
	MTTD / MTR	>280 Days 180+ Days	>200 Days <100 Days	<100 Days 30 Days	Days, Hours, Minutes <7 Days
	Cost	2 x Global average – \$6.2-10M	>Global average \$4.4M-\$6M	<Global average \$2.5-\$4M.	Fraction of global average \$500K - \$1.2M
	Spend	Varying but <3% of IT budget.	5-8% of IT budget	8-10% of IT budget.	8-10% of IT budget.
	Operating Profile	Poor regulatory defense, supply chain DD problematic, Cyber Insurance	Moderate regulatory defense, ad hoc supply chain DD, CI hard	Good regulatory defense, good supply chain DD, CI affordable.	Max regulatory defense, winning supply chain response

Five Questions to Take Away

Each maps to evidence a resilient institution should be able to produce on demand.

If you cannot evidence the answer, the capability is not operational.

