

Securing the digital frontier From defence to value creation.

Next-Generation CISO in a volatile world

Debbie Janeczek – Global CISO

12 November 2025

Ransomware Attack Strikes U.S. Meat Operations at JBS

NOVEMBER 4, 2025

- "SleepyDuck" uses Ethereum for command server
- SesameOp abuses OpenAI Assistants API
- Organized crime cybercrooks steal cargo

Cyber Security Headlines



THE RISE OF AI-POWERED CYBER ATTACK IN 2025

Cybercriminals are increasingly using AI to launch sophisticated and large-scale attacks.



PHISHING EMAILS

AI is generating convincing phishing emails that are personalized and more difficult to detect

DEEPFAKES



ANDY GREENBERG SECURITY JUN 2, 2017 3:30 PM

Hack Brief: Dangerous 'Fireball' Adware Infects a Quarter Billion PCs

A widespread adware infection hides the ability to inflict far worse than spammy browser tweaks.



on networks and systems

AI is creating new strains of malware and ransomware that can adapt to evade security measures

Hosting provider SmarterASP ransomware attack

Majority of customers don't have access to their data

Ransom Refus

State-Owned Pemex Still Recovering From Attack

Spanish IT firm infected with ransomware in continued attacks on supply chains

Hospitals hit by ransomware attacks are seeing an increase in heart patients' death rates



The digital frontier is no longer just about building stronger walls – the walls are permeable, the actor is adaptive, the domain is global.

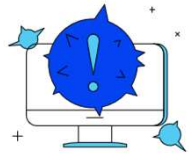
Defend



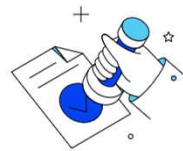
Evolve



Why “defence alone” is no longer sufficient



**Geopolitical
volatility**



**Digital sovereignty
and regulation**



**AI-driven
threats**

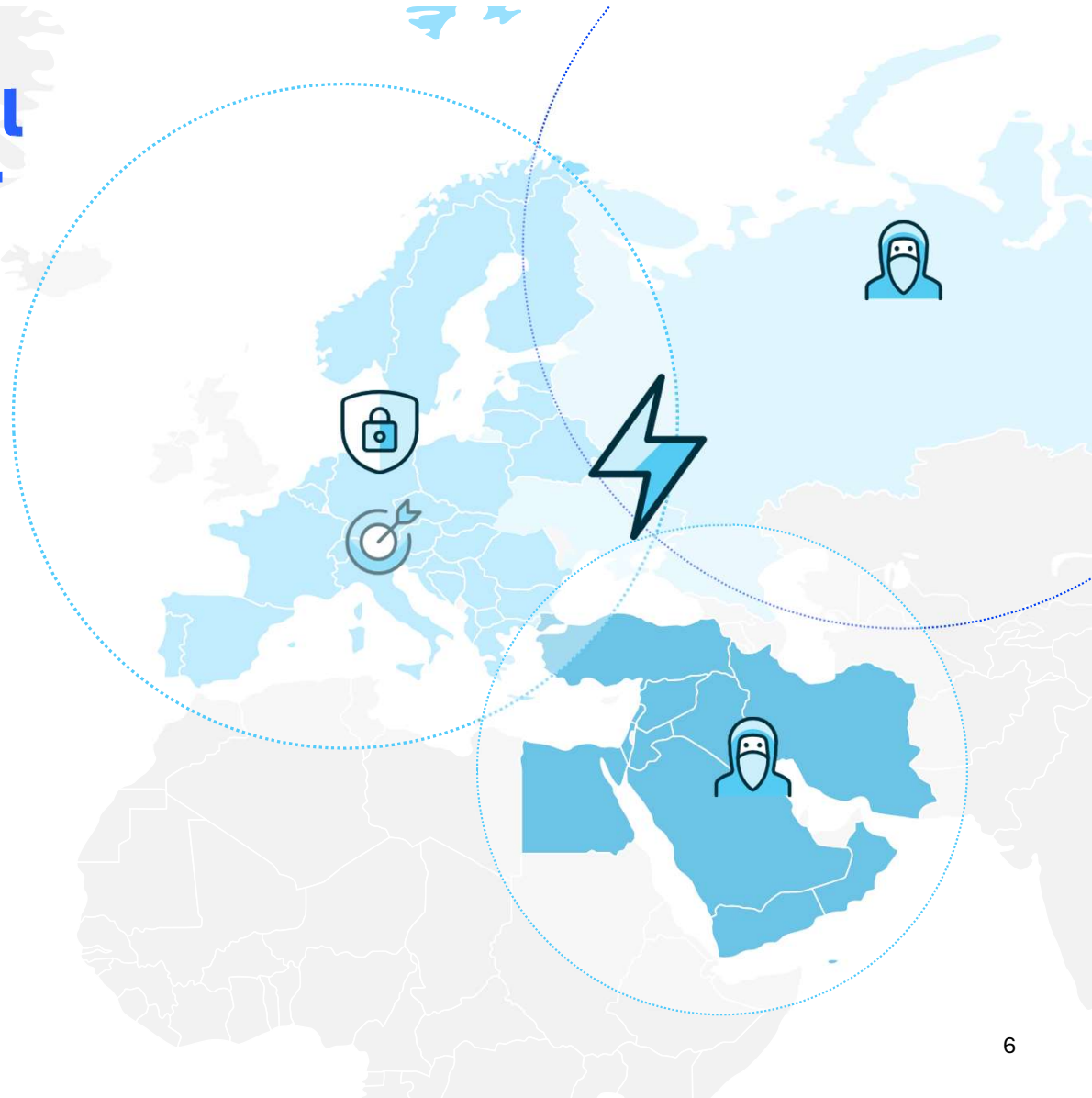
The background is a dark blue field filled with abstract digital patterns. It features numerous vertical lines of varying lengths, each composed of small, glowing blue dots. These lines are interspersed with horizontal, wavy lines that also consist of small blue dots. The overall effect is a sense of depth and complexity, reminiscent of a data visualization or a digital landscape.

01

The evolving threat & risk landscape

Geopolitical and digital sovereignty risk vector

- Geopolitics (nation-states, supply-chain disruption, sanctions) feed cyber risk.
- Digital sovereignty: regulators in many jurisdictions now demand domestic controls, data residency, forced localisation — which complicates global organisations



AI driven threats & adversary advantage

- Threat actor speed, precision, volume: AI/ML tools for attackers, automation, deepfakes, large-scale phishing, AI-powered reconnaissance.
- The challenge: defenders often still operate in slower cycles.
- The “next-gen CISO” must master AI both as threat and defence.



Regulatory and compliance complexity

- Digital sovereignty/regulation (e.g., data localisation, cross-border flows, critical infrastructure regulation).
- Increasing accountability (for CISOs themselves) and expectations for business resilience.
- The convergence of business risk, regulatory risk and cyber risk.



From defence to value creation



Traditional

= Cost centre

Next-gen

= value creator

- Move from “pure defence” (protect, detect, respond) to “resilience + value creation”.
- The CISO must demonstrate how security enables growth, trust, innovation.
- Transition: what capabilities now matter?

The background is a dark blue field filled with abstract digital patterns. It features numerous vertical lines of varying lengths, each composed of small, glowing blue dots. These lines are interspersed with horizontal, wavy lines that also consist of small blue dots. The overall effect is a sense of data flow and digital connectivity.

02

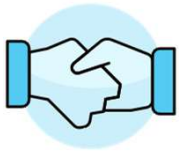
The Next-Generation CISO: capabilities & mindset

Defining “Next-generation CISO”



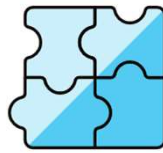
A leader who is strategic (not only technical),
cross-disciplinary (not just IT/security),
deeply connected (internally and externally across ecosystems).

Three foundational mindsets



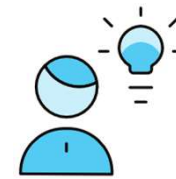
Mindset 1: **Strategic business partner**

Speak business language, translate cyber risk into business terms, drive investments aligned with enterprise goals.



Mindset 2: **Ecosystem orchestrator**

Build alliances across functions (legal, compliance, risk, operations), across vendors/third-parties, across geopolitical/regional nodes.



Mindset 3: **Innovation enabler & resilience driver**

Shift security from blocker to enabler, protect while enabling growth; build adaptive resilience not just hardened defence.



Critical capabilities

Part 1: strategic & business acumen

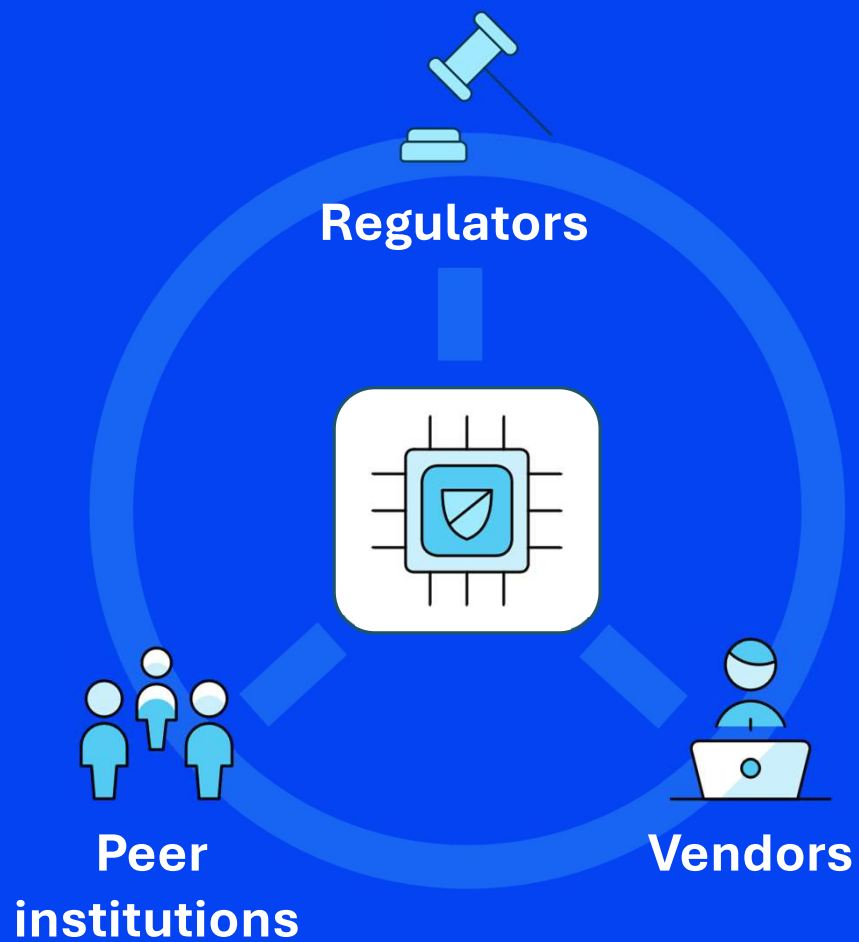
- Ability to articulate cyber risk in financial terms, align with business strategy.
- Board-level communication, executive presence: moving from technologist to leader.
- Decision-making under uncertainty (geopolitical, regulatory, technological).



Critical capabilities

Part 2: Cross-disciplinary leadership

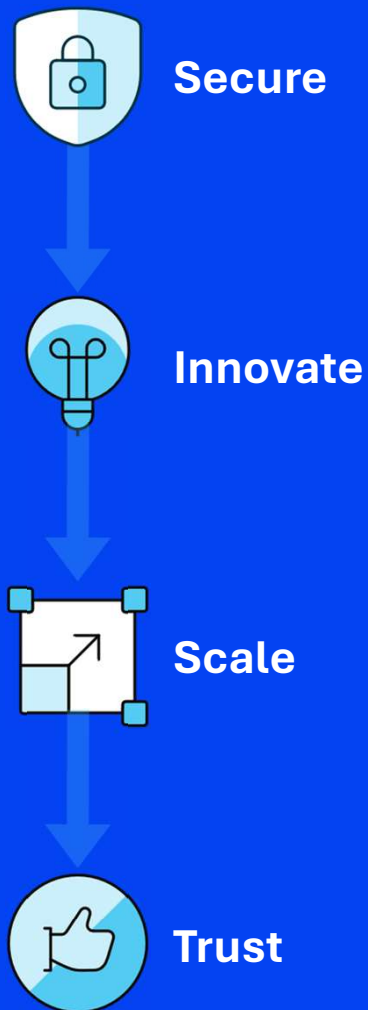
- Build and lead teams across domains (IT, OT, third-party, cloud, legal, compliance).
- Manage vendor/third-party ecosystems (risk and value).
- Collaborate with business functions (product, digital, M&A, transformation).



Critical capabilities

Part 3: Eco system connectivity & resilience

- Establish threat intelligence, red team, insider threat, supply-chain risk functions.
- Foster cooperation: internal (lines of business) and external (industry peers, regulators, law enforcement, cross-border).
- Build resilient architecture: assume breach, design for recovery, digital sovereignty compliance.



Critical capabilities

Part 4: innovation & value creation mindset

- Use security investments to enable new business models, digital trust, customer assurance.
- Example: secure by design product launches, digital transformation with built-in security, enabling M&A with security due-diligence as enabler.
- Reference: CISOs shifting from protection to value driver.

03

Balancing resilience and innovation in a globally complex environment

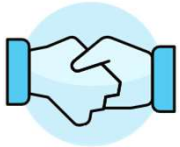
The tension between resilience and innovation

Resilience

Innovation

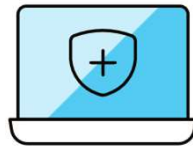
- **On one hand:** need strong controls, compliance, continuity, sovereign data-flows.
- **On the other:** pressure to innovate, go to market fast, scale globally, adopt AI/cloud.
- **The next-gen CISO must balance both**
– not default to blocking innovation.

Framework for balancing – three domains



Domain 1: **Risk governance**

Risk governance & assurance – compliance, resilience, threat-management.



Domain 2: **Transformation enablement**

Digital transformation enablement – embedding security early in product/dev/ops, enabling AI-driven business.

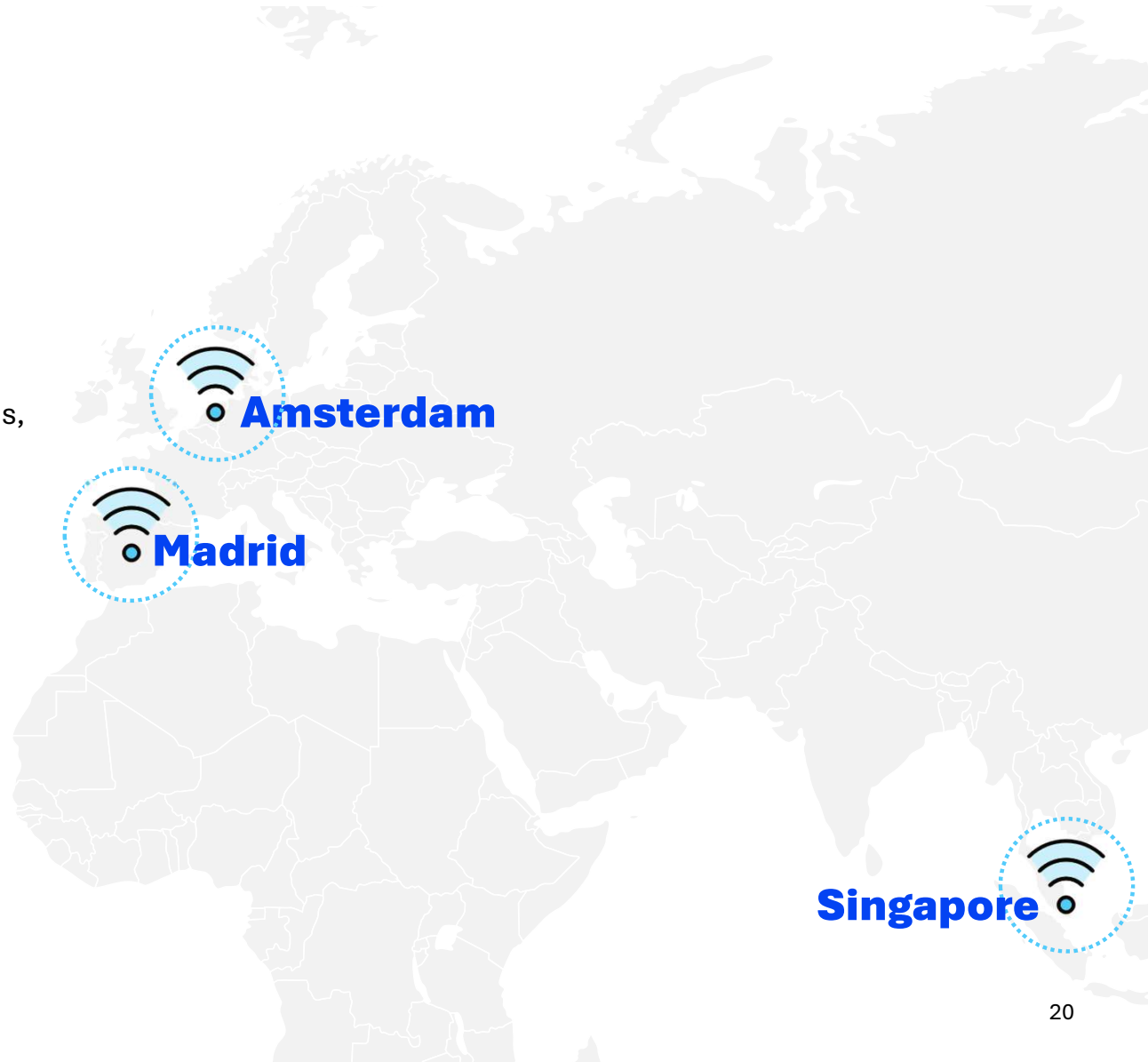


Domain 3: **Global/regulatory strategy**

Global/regulatory/geopolitical view – adapting to local-sovereignty demands, supply-chain disruptions, multi-jurisdictional operations.

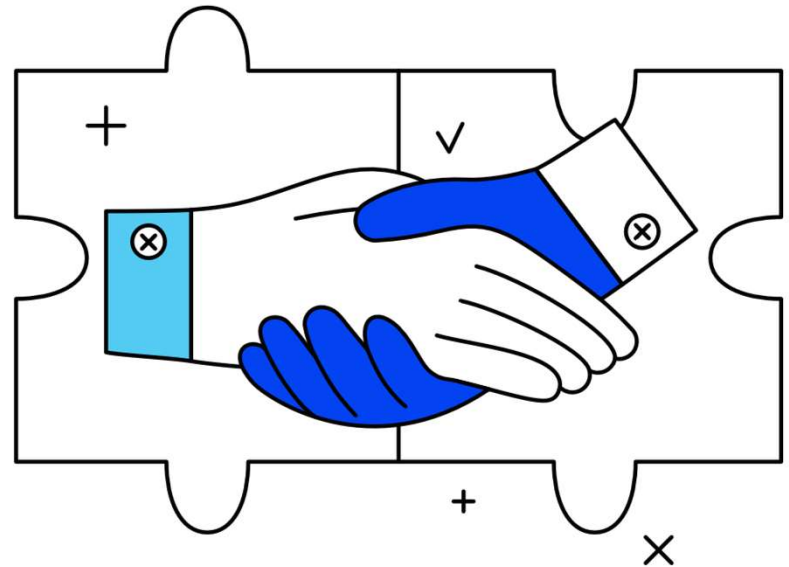
Example case

- Global hub in Madrid, multiple country domains, digital sovereignty pressures, AI adoption.
- Maintaining resilience while enabling business
- Consider your own context



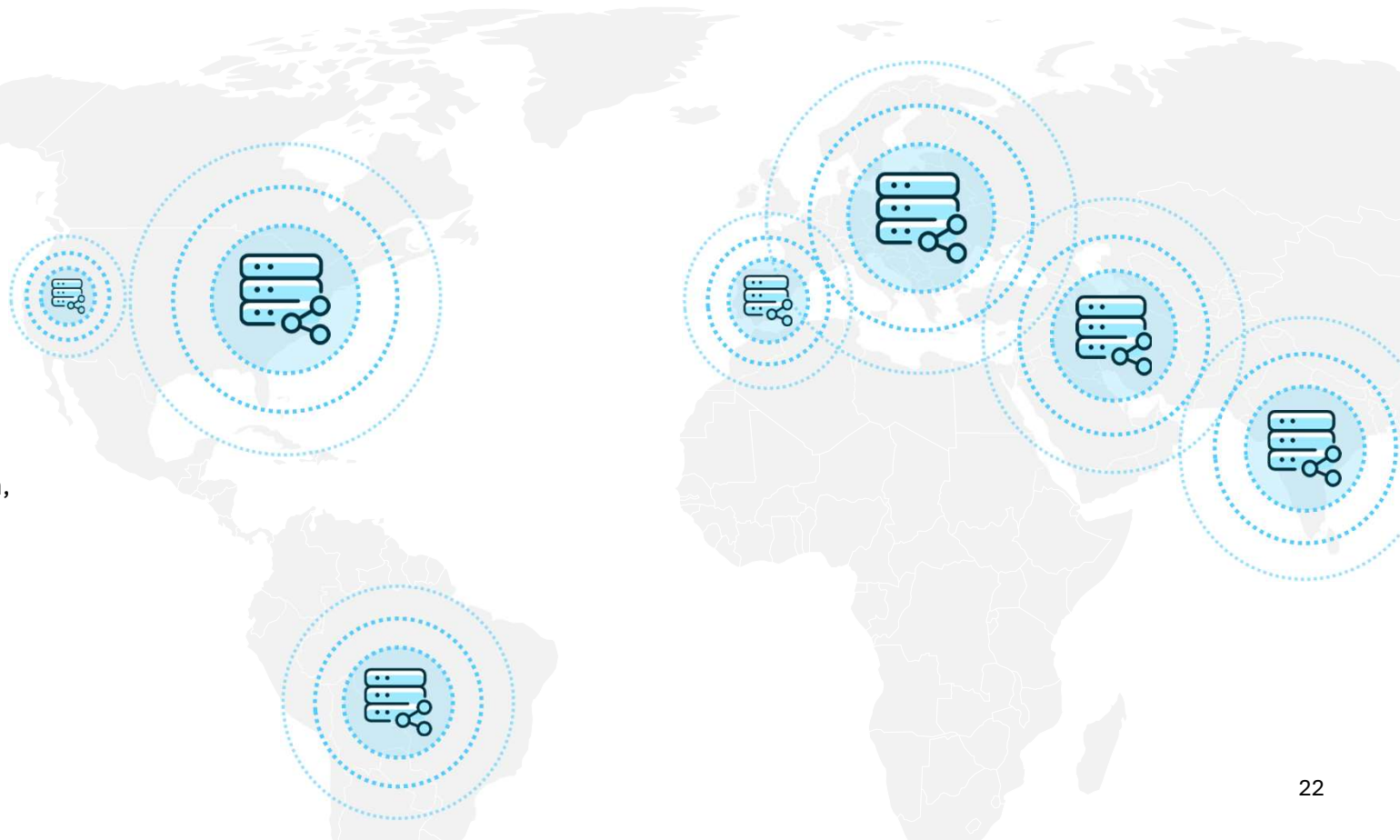
Ecosystem cooperation & partnerships as force-multiplier

- Security can no longer be siloed: share threat intelligence with peers, collaborate with regulators, engage third-party ecosystems.
- Example: industry ISACs, cross-jurisdiction engagements, vendor alliances.
- The next-gen CISO must be networked.



Global complexity & digital sovereignty – practical tactics

- Map regional regulatory demands (data localisation, critical infrastructure regulation, cross-border flows).
- Build regional resilience (e.g., multiple security operations centres, local incident-response capability).
- Incorporate geopolitical risk scenarios (sanctions, supply chain, nation-state ransomware).
- Use this to inform investment, architecture and strategy.



04

**Action plan:
How to get there
& what to prioritise**

Roadmap for next-gen CISO development



Short-Term (0-6 months)

Board briefing refresh
(cyber risk as business risk),
threat-landscape scan
(geopolitics/AI/regulation),
third-party-ecosystem review.



Medium-Term (6-18 months)

Build or mature threat-intelligence
function, embed security in dev/ops,
develop digital sovereignty policy &
architecture, cross-function security
governance forum.



Long-Term (6-18 months)

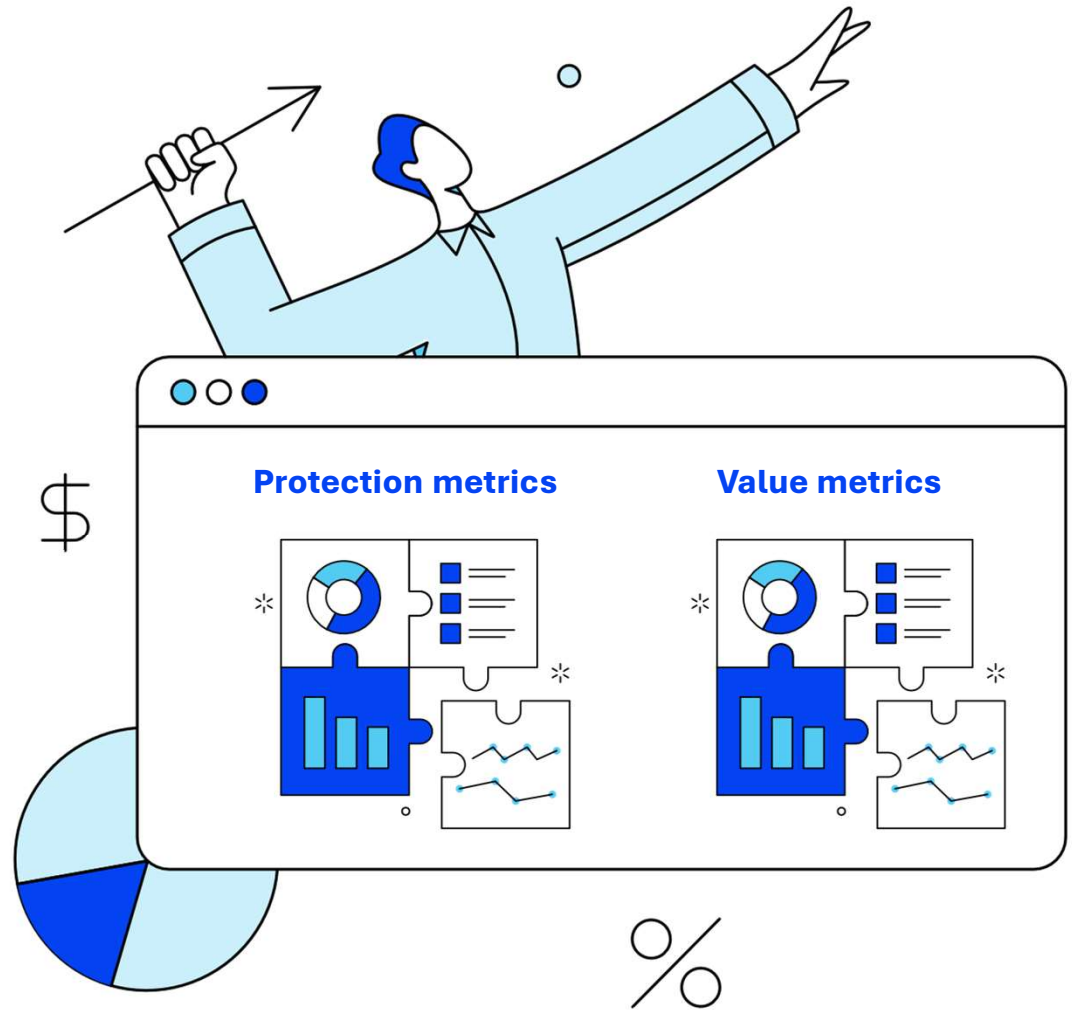
Position security as growth enabler,
derive metrics of value creation
(customer trust, brand, business
enablement), global resilient
architecture, future-tech readiness
(post-quantum, AI adversary
modelling).

Key metrics & KPIs for the next-gen CISO

Traditional: time to detect/respond, number of incidents, compliance status.

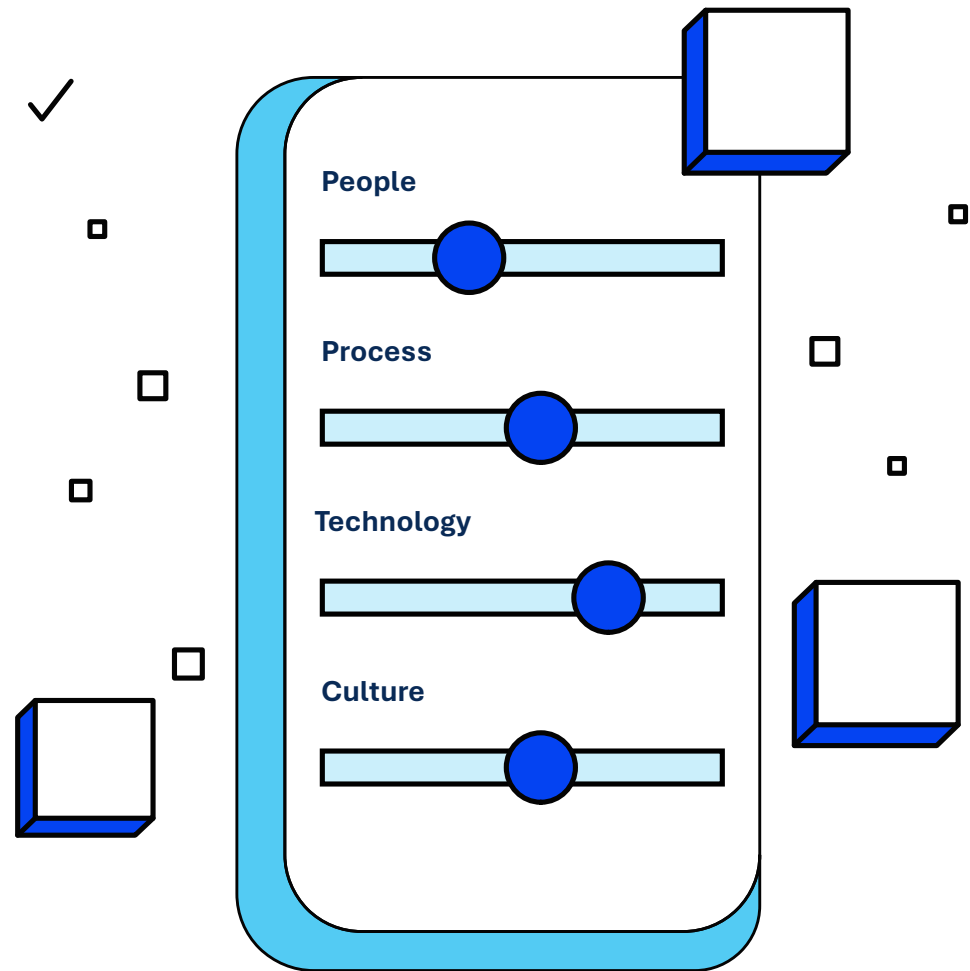
Next-gen: cyber risk in financial terms, business-enabled features launched securely, reduction in time-to-market for secure product, third-party ecosystem risk score, resilience-index (mean time to recovery), value creation metrics (e.g., trust score, customer churn due to security, revenue enabled by secure platform).

Emphasise: metrics must resonate with board & business.



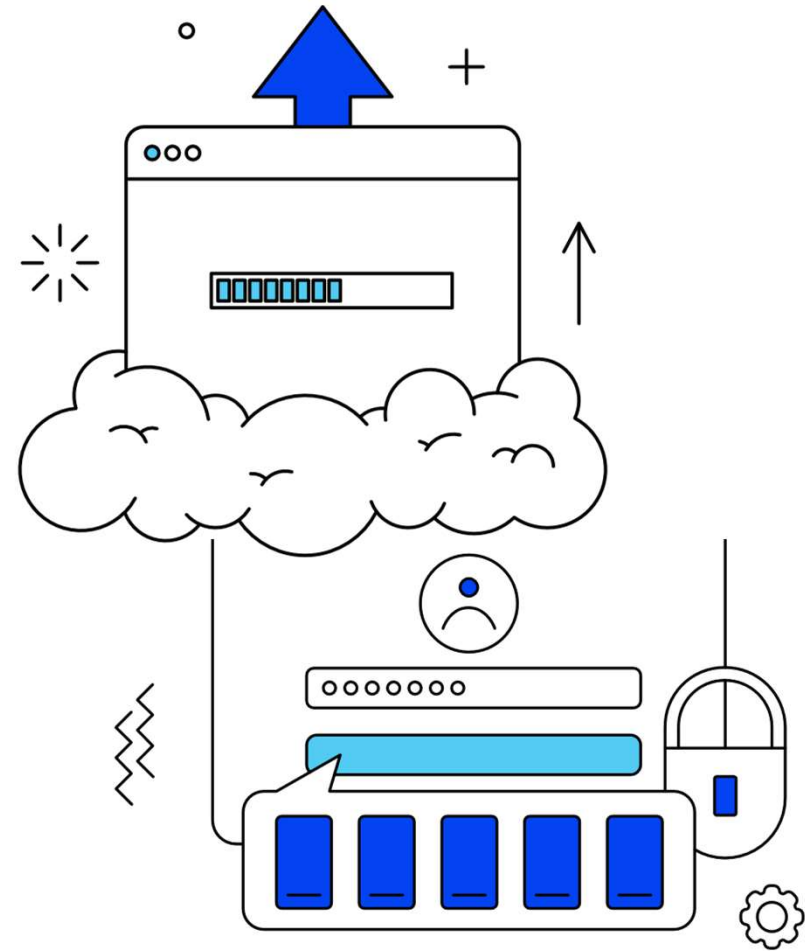
Organisational levers and culture change

- Build security capability (people, process, technology) but also culture: security awareness, risk-centric thinking across business.
- Encourage complexity thinking: friction with rapid innovation must be managed.
- Sponsor from top: you as CISO need executive and board support.
- Internal alignment: security must partner with product, legal, compliance, HR, operations.



Technology & architectural enablers

- Zero-trust, cloud native security, AI/ML for defence and detection, digital sovereignty architecture (data centres, regional segmentation).
- Emerging: post-quantum cryptography, adversarial-AI readiness, supply-chain visibility.
- Note: technology is enabler, but leadership/capability & ecosystem are the differentiator.



Your agenda as CISO

01

Translate cyber risk into business value – speak the language of outcomes.

02

Build a federated ecosystem – align global, local, and third-party security.

03

Embed security into innovation lifecycles – shift left in every project.

04

Design for global complexity – anticipate sovereignty, regulation, and geopolitics.

05

Measure and communicate value creation, not just incident reduction.

Summary

Evolving from protector to value-creator

Recap: The environment has changed; threats are faster, smarter, global.

The role of the CISO must evolve: strategic, connected, enabler of innovation AND resilience.

You must balance defence with value creation, and internal focus with external ecosystem.

“In this volatile world, the CISO is not just the guard at the gate – they are the architect of trust, the enabler of business, the orchestrator of resilience.”

Thank you!