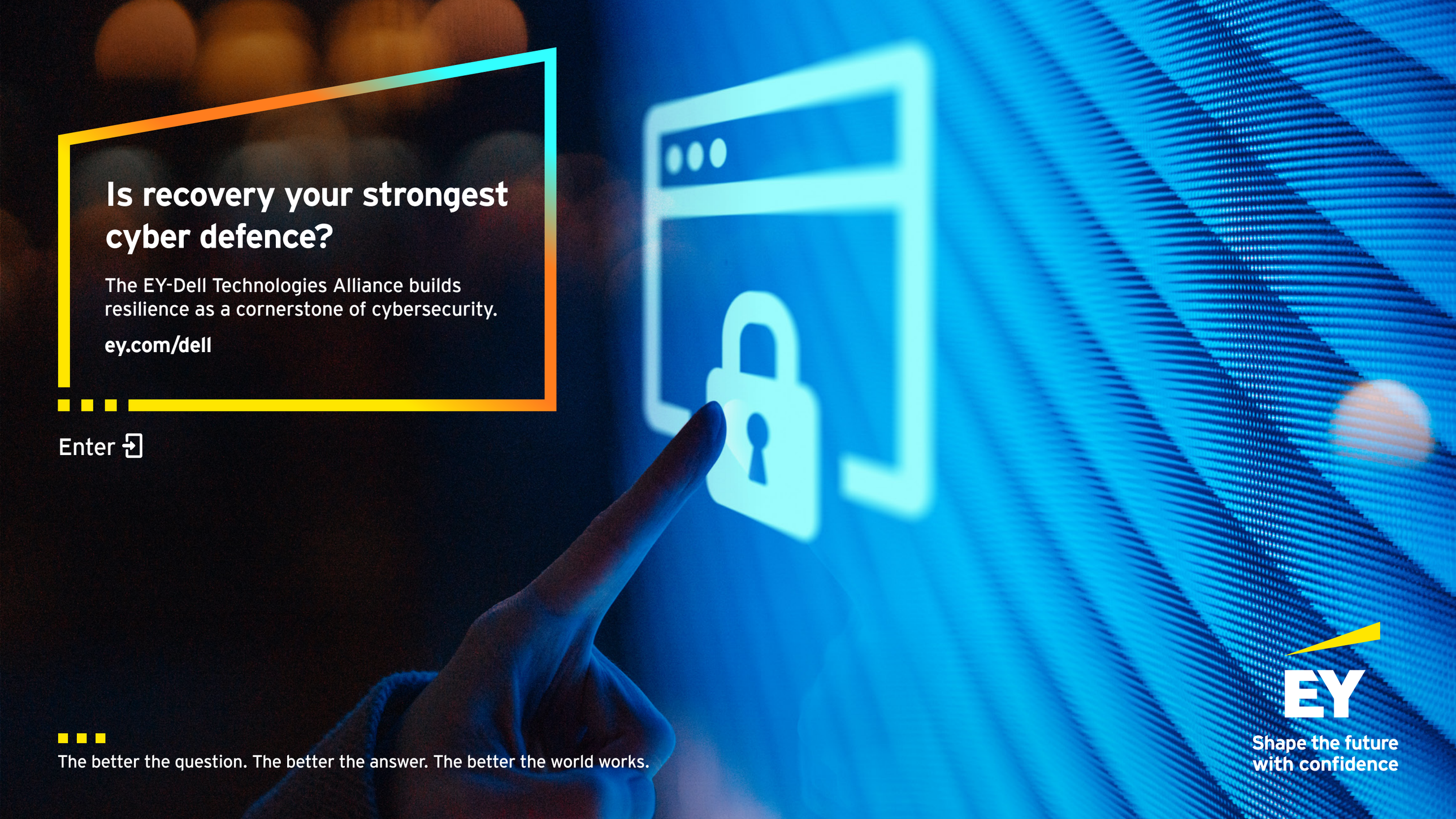
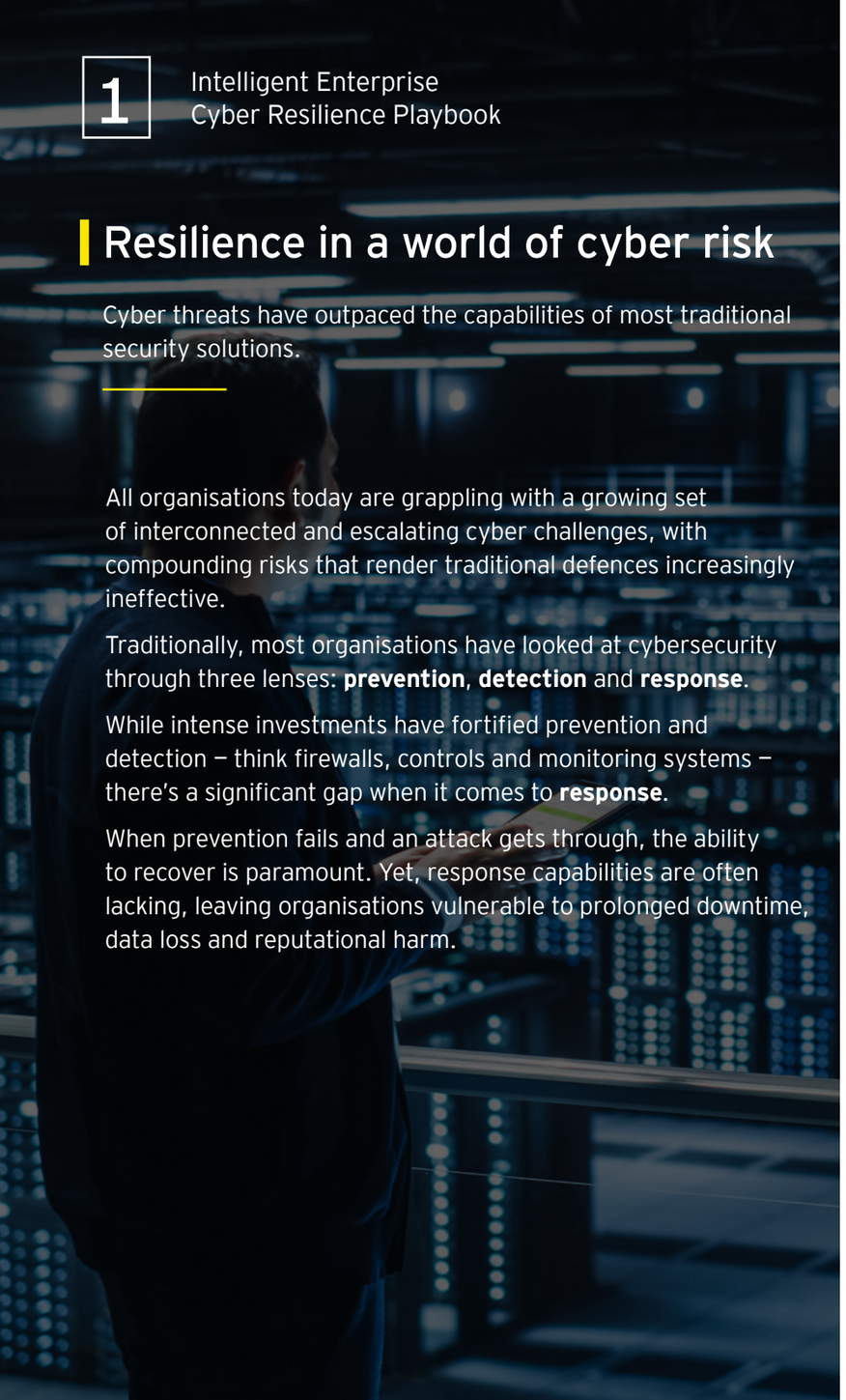

Is recovery your strongest cyber defence?
The EY-Dell Technologies Alliance builds resilience as a cornerstone of cybersecurity.
ey.com/dell
Enter
The better the question. The better the answer. The better the world works.
EY
Shape the future with confidence

Contents

1	Resilience in a world of cyber risk	03
2	By the numbers: cyber risks rise	04
3	CPS 230 means facing the storm together	06
4	Cloudy with a chance of risk	07
5	EY – Dell alliance for resilience	08
6	From crisis to continuity	09
7	What makes the IECR solution unique?	10
8	Shaping the future with confidence	12

Resilience in a world of cyber risk

Cyber threats have outpaced the capabilities of most traditional security solutions.



All organisations today are grappling with a growing set of interconnected and escalating cyber challenges, with compounding risks that render traditional defences increasingly ineffective.

Traditionally, most organisations have looked at cybersecurity through three lenses: **prevention**, **detection** and **response**.

While intense investments have fortified prevention and detection — think firewalls, controls and monitoring systems — there's a significant gap when it comes to **response**.

When prevention fails and an attack gets through, the ability to recover is paramount. Yet, response capabilities are often lacking, leaving organisations vulnerable to prolonged downtime, data loss and reputational harm.

A five-fold challenge

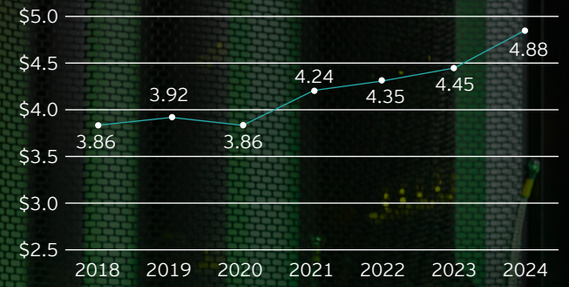
1. **Complex and siloed systems:** Large companies can juggle up to 100 security products from up to 35 providers. These systems are all too often poorly integrated, hard to maintain and lacking a unified view, leaving vulnerabilities exposed.[1]
2. **Delayed response time:** 76% of organisations take six months or longer to detect and respond to cyber incidents, amplifying the damage and delaying recovery.[2]
3. **Escalating costs:** The average cost of a data breach surged to US$4.88 million in 2024 — a 10% rise in just one year.[3] Besides financial cost, the impact of outages on people's lives and essential services they rely on is immense.
4. **Advanced adversaries:** Cybercrime is set to inflict US$10.5 trillion in global damages by 2025, nearly tripling from 2015 levels as sophisticated attackers harness evolving technology.[4]
5. **Constant threats:** Organisations face an average of 44 significant cyber incidents annually, creating a relentless need for robust protection and rapid response mechanisms.[5]

> "An intelligent cyber recovery (ICR) solution is not just a safety net; it is the linchpin of business continuity.

By the numbers: cyber risks rise

Data breach costs climb

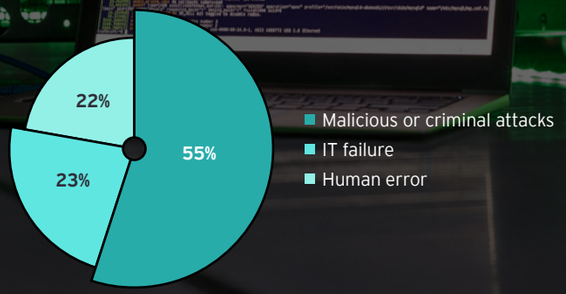
Global average total cost of a data breach



Source: IBM, 2024.

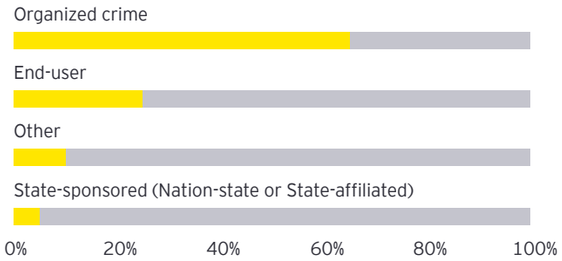
Cybercrime is big business

Root cause of the data breach between 3 categories



Source: IBM, 2024.

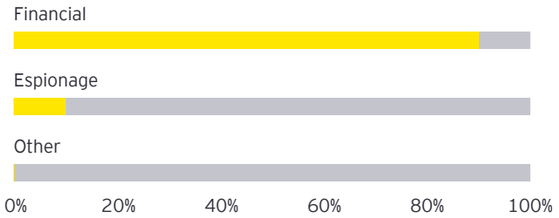
Cybercrime is big business



Threat actor varieties in breaches (n=7,921)

Source: Verizon, 2024.

Attack motives are clear



Threat actor motives in breaches (n=5,632)

Source: Verizon, 2024.

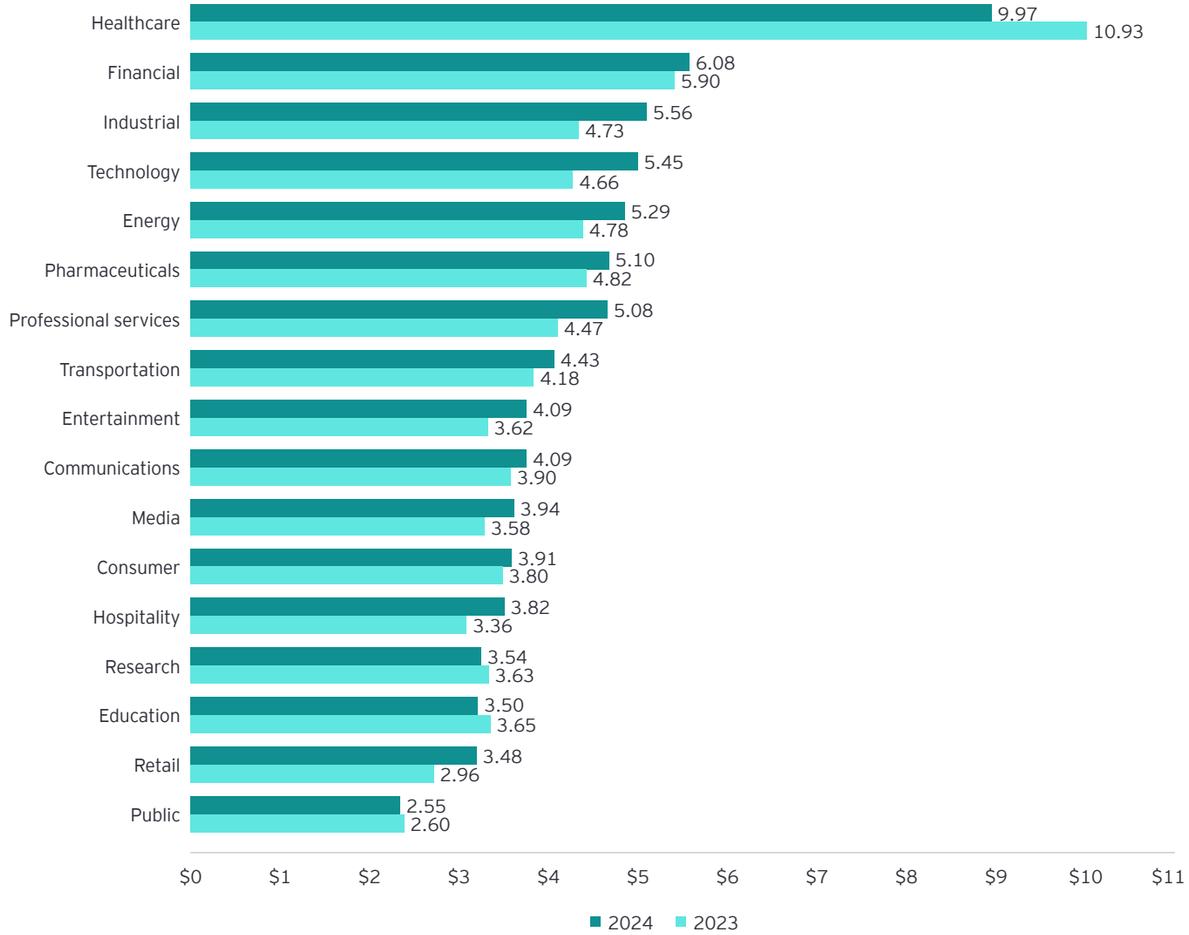
Ransomware attacks are spiralling, and backup repositories are in the line of fire

Increase of **73%** in ransomeware attacks from 2022 to 2023[1]	Backup repositories are targeted in **96%** of attacks[2]	Ransom payment represented **32%** of the total financial impact of ransomeware[2]
Average ransom payment was **$381 980** in Q1 2024[3]	Average time-to-recover recover was **3.4 weeks** after a ransomeware attack[4]	More than **317m** ransomeware attempts in 2023[5]

1. eCrime.ch – Threat and Risk intelligence Services
2. Veeam Ransomware Trends Report 2024
3. Covewave Quarterly Ransomeware Report
4. Veeam Ransomware Trends Report 2023
5. Statista

Financial services are in cybercriminals' line of sight

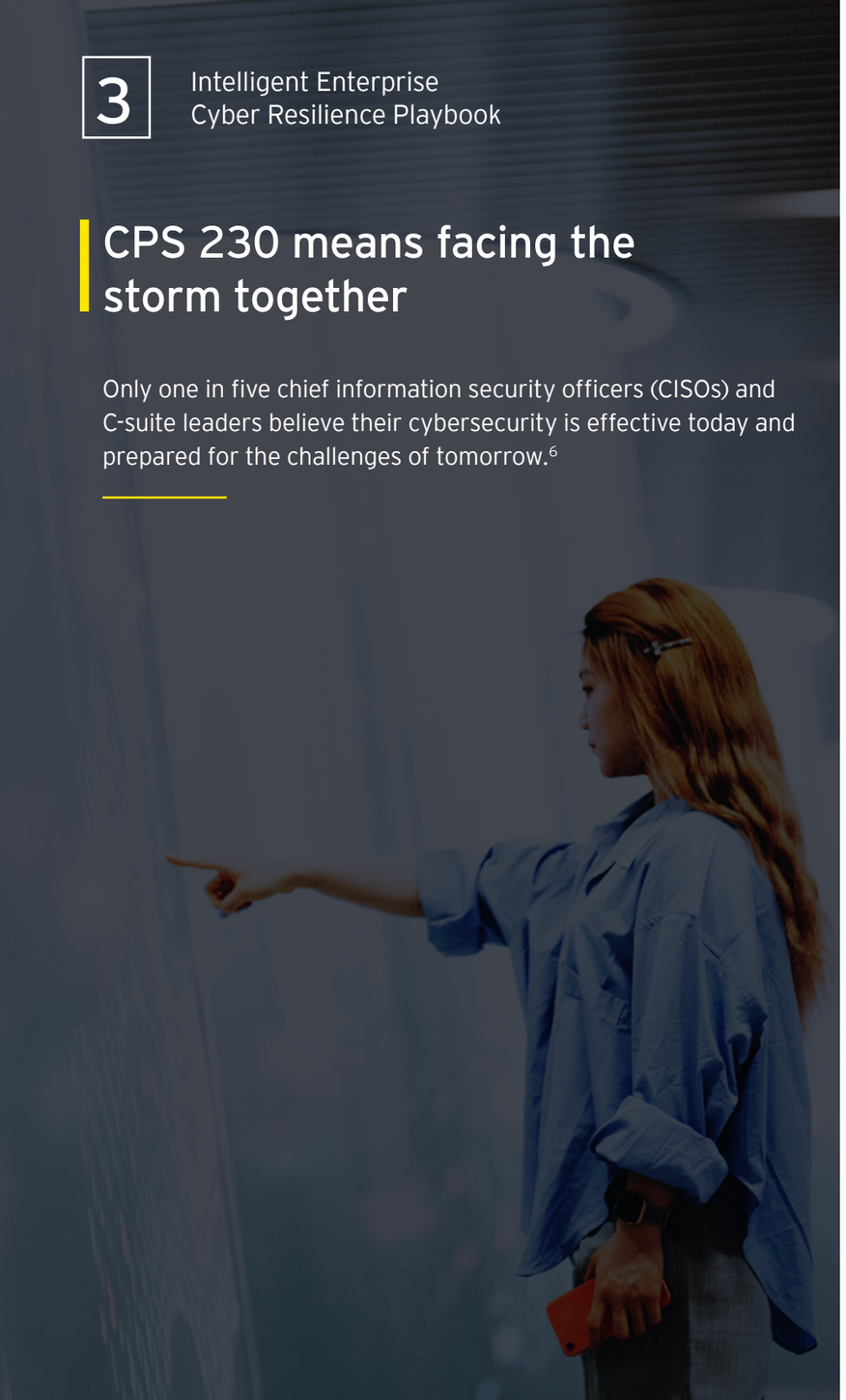
Cost of a data breach by industry



Source: IBM, 2024.

CPS 230 means facing the storm together

Only one in five chief information security officers (CISOs) and C-suite leaders believe their cybersecurity is effective today and prepared for the challenges of tomorrow.[6]



For financial services, the stakes are sky high. Protecting sensitive data while maintaining compliance in an increasingly hostile cyber landscape demands urgent action.

Cybersecurity isn't just about prevention anymore. CPS 230 mandates that banks, insurers and superannuation trustees make cybersecurity a cornerstone of their operational risk strategies.

CPS 230 prioritises collaboration across business, risk and technology functions and each plays an important role:

- **Business teams** define priorities and identify critical functions
- **Technology teams** build resilient systems and processes
- **Risk and assurance teams** integrate these efforts into a cohesive strategy

While CISOs focus on countering specific threats, the C-suite must adopt a broader approach. The real question is: **Can we trust our systems to protect our business, minimise disruptions and recover quickly when crises hit?**

Facing the cyber storm requires unified action and unwavering confidence in technology, people and processes. CPS 230 is a timely reminder that resilience isn't just compliance – it's a strategic necessity.

Key questions for financial services

- Are we approaching cyber resilience in a holistic way?
- Are we regularly testing cyber recovery plans against the once unthinkable, now plausible and severe scenarios of tomorrow?
- How well-prepared are we to meet advanced Cyber Recovery Point Objectives (CRPO) and Cyber Recovery Time Objectives (CRTO) – and are we closing the critical gaps in our cybersecurity strategy?
- How are we deploying data and AI to continuously monitor and manage the cyber risks associated with our third parties and sub-contractors?

> "With Australia's Prudential Standard CPS 230 Operational Risk Management taking effect on 1 July 2025, financial institutions must rethink how they approach business continuity.

Cloudy with a chance of risk

Back in 2019, Gartner predicted that 80% of enterprises would move away from their traditional data centres by 2025 and migrate to the cloud.[7] Since 2020, Cloud has been in the top two technology priorities for financial services[8].

Since then, the risks of cloud reliance have become all too familiar.

Consider this scenario: a company, fully dependent on its cloud provider to store critical business data, is the target of a ransomware attack. The ransomware spreads rapidly, locking all the company's data – both live and backups – and rendering files encrypted. With no isolated network to contain the damage, even the backups which should serve as a safety net are compromised.

Or imagine this scenario: a financial service company's cloud provider accidentally deletes crucial data during routine maintenance. Without a secure, disconnected backup system, the result is lost data, extended downtime, financial setbacks, regulatory repercussions, and a tarnished reputation.

Had either company implemented an airgap solution, its backup data would have been securely isolated – offering a reliable fallback in the event of an attack or an error, safeguarding operations and business continuity.

> “Companies can't afford to assume their cloud provider has every cyber risk covered. Cloud security is a shared responsibility, particularly around identity and access management. Misconfigurations are all too common, and securing the cloud demands more than a simple 'lift and shift' approach – it requires intentional setup and vigilance.

Rohit Rao
EY Asia-Pacific Financial Services
Cybersecurity Leader

EY – Dell alliance for resilience

Modern cyber threats demand modern solutions.

The EY-Dell Technologies Alliance is helping to create more resilient and futureproof businesses by innovating across the multi-cloud and edge ecosystems.

One powerful solution is the **EY Intelligent Enterprise Cyber Resilience (IECR)**.

IECR brings together the strategic experience of EY teams with the technical acumen of Dell to provide a broad and customised cyber resilience framework.

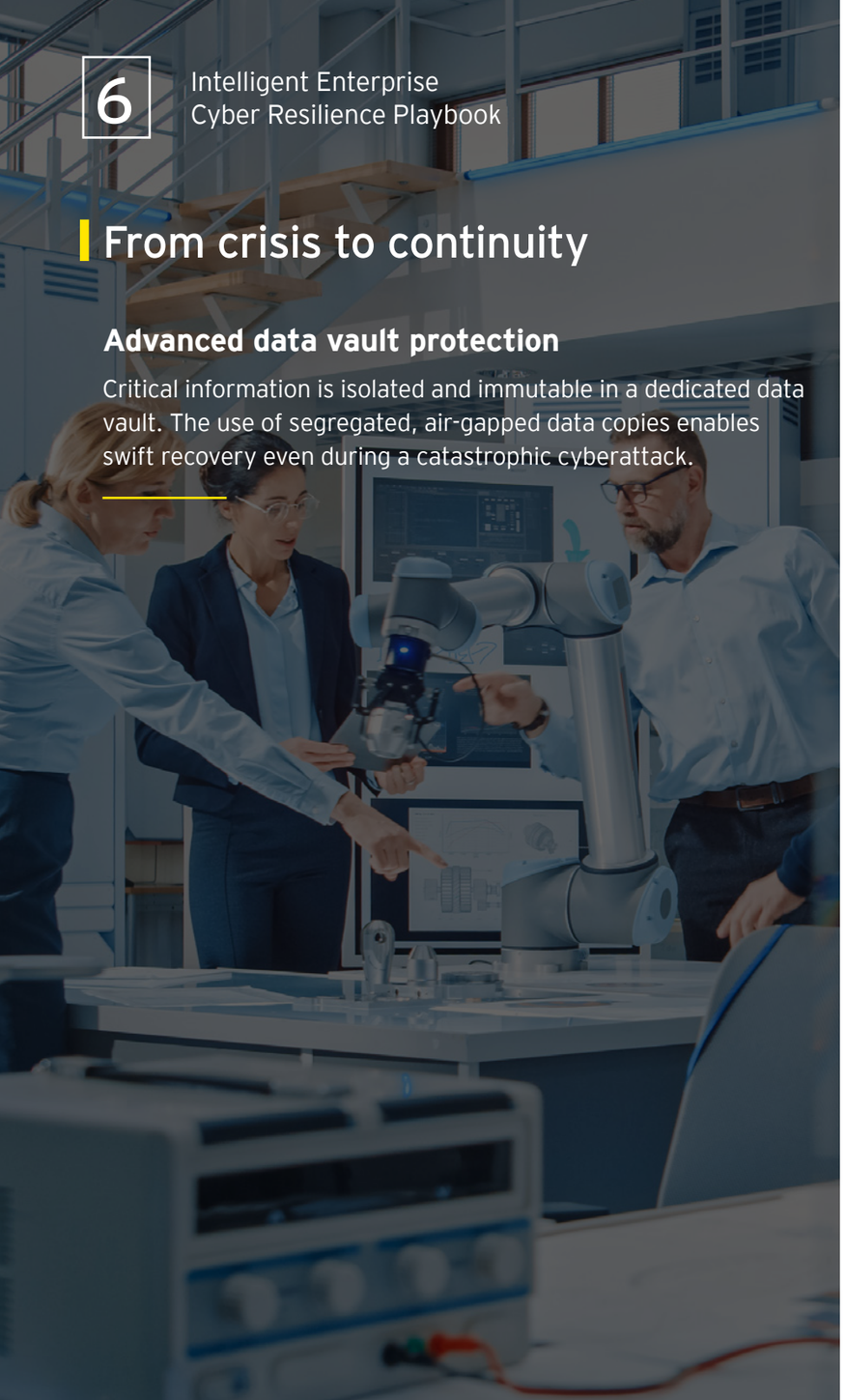
This solution supports rapid restoration of operations during crises, minimising disruptions and reducing the impact on customers and revenue.

It goes beyond the traditional protect-and-respond model, integrating all elements of the National Institute of Standards and Technology (NIST) framework. It is future-focused, AI-enabled, and supports rapid decision-making in crises.

Learn more about the solution.

> “When standing in the eye of a cyber storm, it’s not about saving everything – it’s about saving what matters most. By focusing on Minimal Viable Banking Operations (MVBO), core functions can continue even when systems and processes are disrupted. MVBO allows your customers to keep operating during the crisis, and when the dust settles, your bank can recover faster.

Mayank Joshi
Director, Technology Consulting and Cyber Security, Ernst & Young, Australia



From crisis to continuity

Advanced data vault protection

Critical information is isolated and immutable in a dedicated data vault. The use of segregated, air-gapped data copies enables swift recovery even during a catastrophic cyberattack.

Predictable recovery times

A secure restore and inspection zone ensures data is thoroughly verified and cleaned before being reintegrated into operational systems, minimising downtime.

AI-powered threat detection and recovery

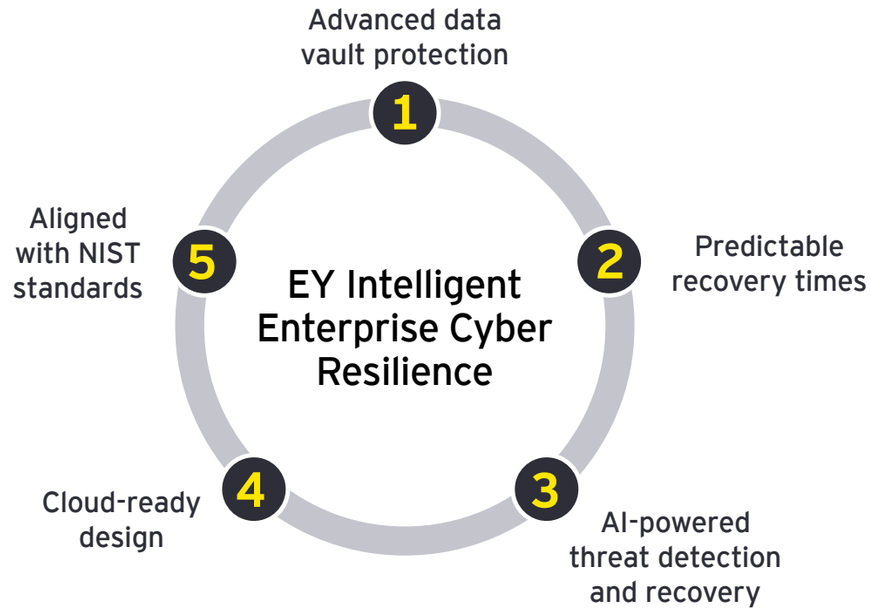
Advanced AI and machine learning analyses vaulted data, detects anomalies and predicts potential cyberattacks. When an attack occurs, AI speeds up critical data recovery.

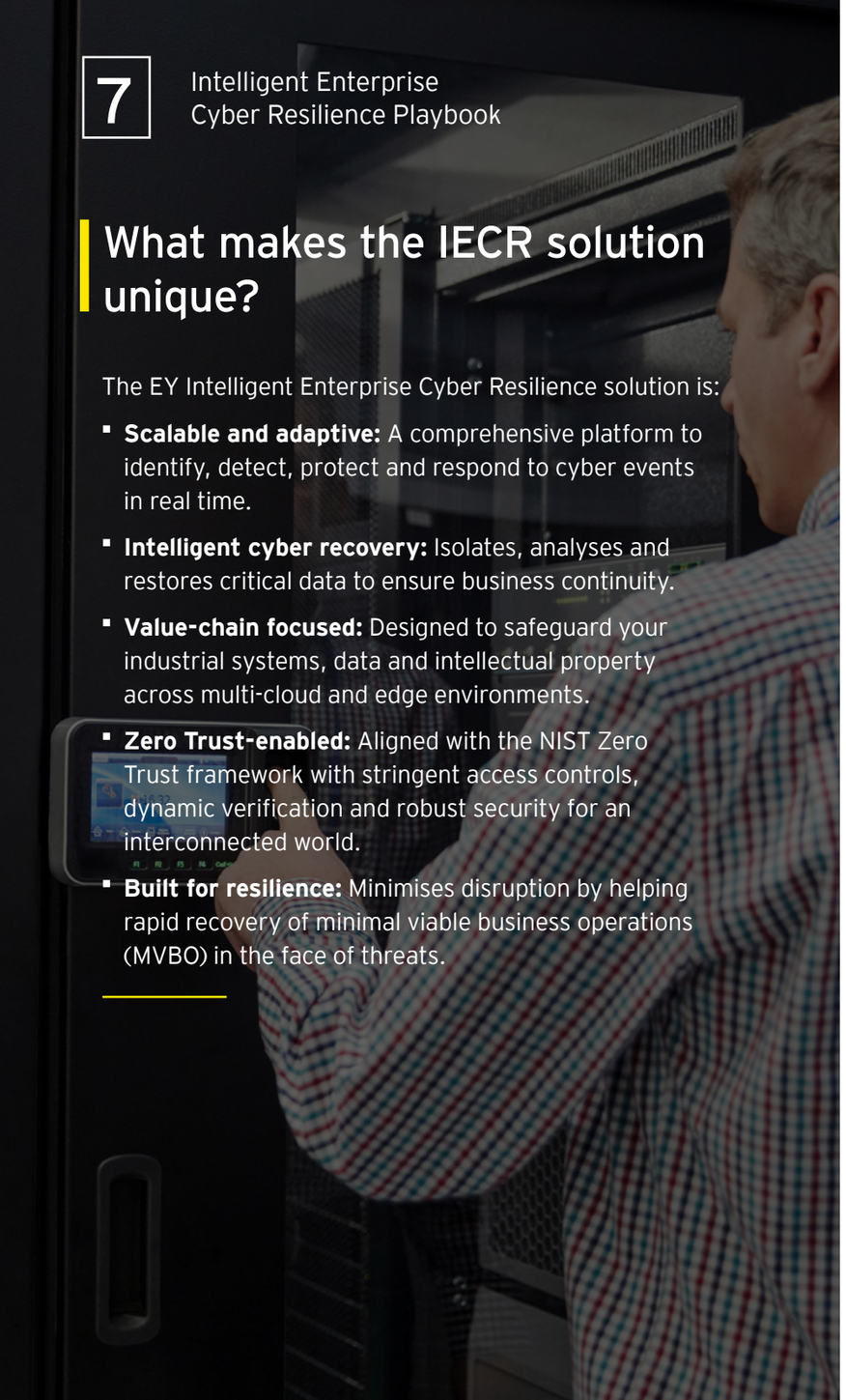
Cloud-ready design

Built with cloud-ready design principles, the solution offers scalability, flexibility and resilience, seamlessly integrating with evolving business needs.

Aligned with NIST standards

IECR adheres to the U.S. National Institute of Standards and Technology (NIST) guidelines, empowering organisations to manage and mitigate risks in alignment with globally recognised leading practices.





What makes the IECR solution unique?

The EY Intelligent Enterprise Cyber Resilience solution is:

- **Scalable and adaptive:** A comprehensive platform to identify, detect, protect and respond to cyber events in real time.
- **Intelligent cyber recovery:** Isolates, analyses and restores critical data to ensure business continuity.
- **Value-chain focused:** Designed to safeguard your industrial systems, data and intellectual property across multi-cloud and edge environments.
- **Zero Trust-enabled:** Aligned with the NIST Zero Trust framework with stringent access controls, dynamic verification and robust security for an interconnected world.
- **Built for resilience:** Minimises disruption by helping rapid recovery of minimal viable business operations (MVBO) in the face of threats.

The EY Intelligent Enterprise Cyber Resilience can help you confidently protect what matters most to your business – your customers.

Stage 1	Stage 2	Stage 3	Stage 4
Scope Cyber Recovery Solution	**Pilot Cyber Recovery Solution**	**Rollout Cyber Recovery Solution**	**Embed Cyber Recovery Solution**
The scoping stage focuses on developing the high-level opportunity and size of the Cyber Recovery Solution. A key aspect of this stage is to build executive awareness and understanding of the solution.	Implementation for a limited set of services The pilot stage aims to design and implement a CRS Minimal Viable product (MVP) for a limited set of services (typically two critical infrastructure services and the client's data production solution).	Phased implementation for all in-scope services The rollout stage builds on the foundation of the pilot stage to scale to all services that have been identified as in scope for the solution.	This stage focuses on operationalisation of the solution in the business.

Cyber recovery maturity assessment ▶ Design solution ▶ Technical and service implementation ▶ Playbook deveopment ▶ Design solution ▶ Technical and service implementation ▶ Playbook deveopment ▶ Crisis and incident management framework

Program, strategy and governance

Securing data, strengthening recovery

Forrester Consulting's Total Economic Impact™ study analysed and built a composite of five companies* with experience using the solution. This study confirms measurable value including:

- **80% faster data recovery:** less time spent by employees locating data to restore.
- **75% less system downtime:** minimising lost employee productivity.
- **Minimal disruptions from reduced downtime:** reducing disruptions to sales, services and reputation damage.
- **Substantial legacy system savings:** retiring outdated backup infrastructure and maintenance costs delivers substantial savings.[9]

*Composite = 1,500 employees and an operating budget of US$500 million experiencing quantified benefits of $463,000 over 3 years versus costs of $US303,000, an ROI of 53%.

Beyond the hard numbers, Forrester uncovered a range of unquantified benefits:

- **Lower insurance costs:** Enhanced resilience reduces insurance risk and premiums.
- **Stronger business resilience:** IECR fosters a proactive security mindset, strengthening overall organisational preparedness.
- **Streamlined audits:** Simplifies compliance, accelerating audit readiness and approval.
- **Boosted employee confidence:** Supports data security and reassures teams their work is protected.

ROI rewards – Forrester example organisation

53%
Return On Investment

$160,000
Net Present Value

53%
reduction in recovery time

18-month
payback.[10]

Shaping the future with confidence

Rohit Rao
EY Asia-Pacific Financial Services
Cybersecurity Leader
rohit.rao@au.ey.com

Mayank Joshi
Director, Cybersecurity and Technology
Consulting, Ernst & Young, Australia
mayank.joshi@au.ey.com

Contact us to schedule a discovery session to explore how the EY-Dell Technologies Alliance can help you to build resilience and empower you to shape the future with confidence.

References

EY and Microsoft. (2023). *How does rationalizing cybersecurity tools enhance security effectiveness and efficiency?*

EY. (October 2023). *Cyber leaders' confidence in their organization's defenses plummets, but costs mount.*

Forrester. (August 2023). *The Total Economic Impact™ of Dell PowerProtect Cyber Recovery.*

Gartner. (August 2019). The Data Center Is (Almost) Dead.

IBM. (2024). *Cost of a Data Breach Report 2024.*

Morgan, S. (October 2023). Cybercrime To Cost The World $9.5 trillion USD annually in 2024. Cybercrime Magazine.

Verizon

Watson, R. (May 2024). How can cybersecurity transform to accelerate value from AI?

[1] EY and Microsoft, 2023. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-us/alliances/documents/ey-how-does-rationalizing-cybersecurity-tools-enhance-security-effectiveness-and-efficiency.pdf

[2] EY, 2023. https://www.ey.com/en_au/newsroom/2023/10/cyber-leaders-confidence-in-their-organizations-defenses-plummets-but-costs-mount

[3] IBM, 2024. https://www.ibm.com/reports/data-breach

[4] Morgan, 2023. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[5] EY, 2023. https://www.ey.com/en_au/newsroom/2023/10/cyber-leaders-confidence-in-their-organizations-defenses-plummets-but-costs-mount

[6] Watson, 2024. https://www.ey.com/en_gl/ciso

[7] Gartner, 2019. https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead

[8] EY, 2022, Tech Horizon 2022: How to build a data-centric organization | EY - Global | EY - Global

[9] Forrester, 2023.

[10] Forrester, 2023.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYSCORE 001290-25-AUNZ

BMC Agency
GA 141628606

ED None

ey.com