happiest minds
AI FIRST. AGILE ALWAYS.

BUSINESS RESILIENCY

RESILIENCE THAT POWERS GROWTH

> Resilience is not a cost - it is your competitive moat.

$9,000/min
Peak Downtime Cost
Ponemon Inst., 2026

Up to 4% ARR
Regulatory Fines Risk
DORA / GDPR, 2025

3 - 8×
Resilience ROI per $1
Industry benchmark

24 days
Avg. Ransomware Recovery
Verizon DBIR, 2025

TABLE OF CONTENTS

01

EXECUTIVE SUMMARY

Business Resiliency is no longer a back-office IT discipline. It is the operating condition that determines whether an enterprise survives disruption - or becomes a cautionary statistic in the next industry report.

In the two decades I have spent in infrastructure and consulting, I have watched organizations oscillate between two failure modes: investing too little in resilience until a crisis forces their hand or investing without structure - patching individual gaps without building coherent capability. Both are expensive. Both are avoidable.

The threat environment of 2026 is materially different from even two years ago. Ransomware attacks increased 105% year-over-year in 2025. AI is now weaponized by adversaries at a speed that outpaces traditional defences. DORA became enforceable in January 2025, and regulators have moved from reviewing frameworks to demanding operational proof. The cost of inaction - $4.44M per breach on average, 24 days of ransomware recovery, potential fines up to 4% of annual revenue - dwarfs any investment in structured resilience.

> **The enterprises that recover fastest from disruption are not the ones with the biggest IT budgets. They are the ones that treated resilience as an operating discipline before the crisis arrived. When a ransomware attack hits at 2 a.m. on a Friday, the only thing that matters is whether your runbooks exist, your backups are verified, and your team knows exactly what to do next.**
>
> **Rambabu Pothu**
> Global Consulting & Implementation Head, IMSS

This whitepaper presents the strategic case for a structured, enterprise-wide Business Resiliency program, and the AI-led methodology Happiest Minds uses to build, benchmark, and continuously improve it. It is not a compliance checklist. It is a practical operating framework designed for enterprises that want resilience to be a source of competitive advantage - not just a risk mitigation measure.

KEY TAKEAWAY

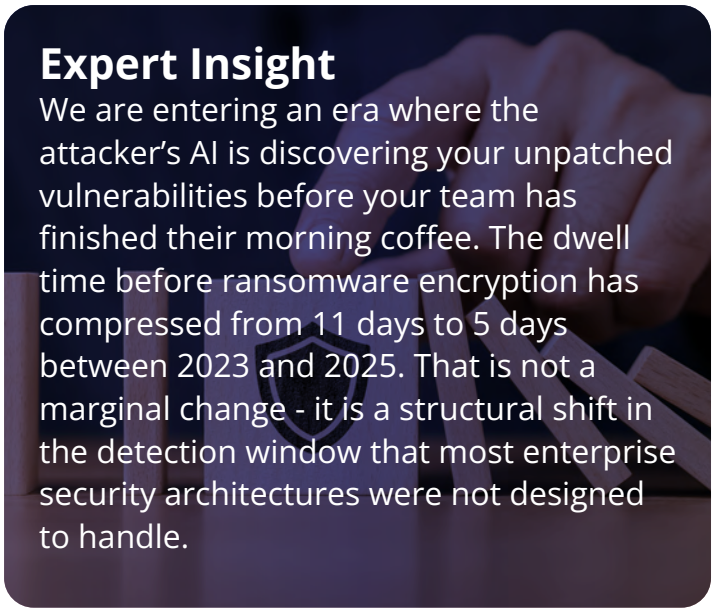
Organizations that embed resilience into their operating model - not just their IT policy - recover 3–8× faster, face significantly fewer regulatory penalties, and retain customer trust when disruption strikes.

THE 2026 ENTERPRISE RISK LANDSCAPE

Four macro-forces have converged to create a threat environment of unprecedented complexity. Understanding each one is the prerequisite for building a resilience program that actually holds under pressure.

2.1 AI-Powered Threat Actors

The most significant shift I have observed in the past 18 months is the weaponisation of AI by adversaries. This is not theoretical. Microsoft's 2025 Threat Intelligence Report documented AI-assisted cyberattacks across at least four nation-state actors, with automated vulnerability exploitation running faster than any human security team can manually respond.



Expert Insight

We are entering an era where the attacker's AI is discovering your unpatched vulnerabilities before your team has finished their morning coffee. The dwell time before ransomware encryption has compressed from 11 days to 5 days between 2023 and 2025. That is not a marginal change - it is a structural shift in the detection window that most enterprise security architectures were not designed to handle.

Ransomware groups are now deploying AI-generated deepfake voice calls for social engineering, polymorphic malware that evades signature detection, and automated phishing at industrial scale. The human element - the employee who receives a call that sounds exactly like their CFO - has become the primary attack surface in ways that technical controls alone cannot fully address.

How are AI-powered cyberattacks different from traditional ransomware?

?

Traditional ransomware relied on known exploit kits and manual targeting. AI-powered attacks automate vulnerability discovery, generate convincing social engineering content (including deepfake voice and video), adapt malware signatures in real time to evade detection, and compress the attack lifecycle from weeks to days. The 2025 dwell time before encryption dropped to 5 days - leaving a fraction of the detection window enterprises previously had.

2.2 **Ransomware:** An Industrialized Business Model

Ransomware-as-a-Service (RaaS) has democratized cybercrime. GuidePoint Research counted 124 active ransomware groups in 2025 - up 46% year-over-year - with less technically skilled actors launching sophisticated campaigns using off-the-shelf attack infrastructure.

The CDK Global attack in June 2024 paralysed operations at over 15,000 automotive dealerships and generated more than $1 billion in downstream losses - a single supply-chain-adjacent breach with systemic consequences. In 2025, 55% of enterprise CISOs reported facing at least one cyberattack, with recovery costs averaging $5 million per incident.

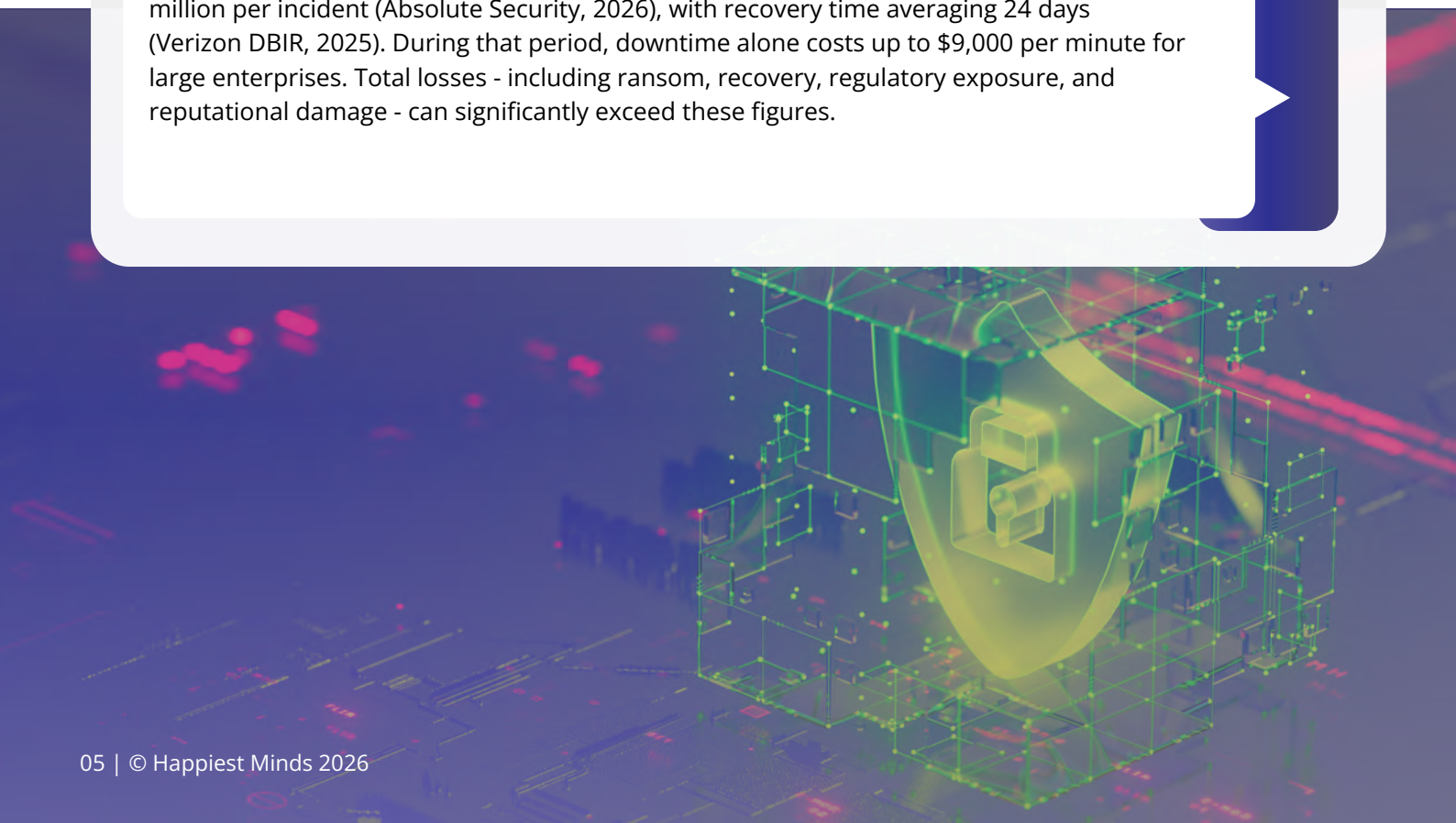
Expert Insight

What strikes me about the CDK Global incident is not the scale of the attack itself - it is what it revealed about dependency mapping. Thousands of dealerships had no visibility into how deeply CDK's systems were woven into their daily operations until everything stopped. The lesson is not to diversify vendors. The lesson is to know your dependency graph before the attacker exploits it.

What is the average cost of a ransomware attack on an enterprise?

?

In 2025, the average ransomware recovery cost for enterprise organizations reached $5 million per incident (Absolute Security, 2026), with recovery time averaging 24 days (Verizon DBIR, 2025). During that period, downtime alone costs up to $9,000 per minute for large enterprises. Total losses - including ransom, recovery, regulatory exposure, and reputational damage - can significantly exceed these figures.



2.3 Regulatory Tightening: From Advisory to Enforceable

DORA became enforceable in January 2025. In 2026, regulators have moved from reviewing policies to demanding operational proof - real-time evidence of resilience in practice, not just on paper. For global enterprises, this shift is consequential even outside the EU: non-EU technology providers serving EU financial clients must also demonstrate DORA compliance.

Expert Insight

I advise clients to stop thinking of DORA as a compliance project and start thinking of it as a business transformation. The organizations that treat it as a box-ticking exercise are the ones that will face the most painful supervisory engagement in 2026. The regulation is not asking you to be perfect. It is asking you to demonstrate that you know what your risks are, that you can detect incidents quickly, and that you have tested your recovery. That is a reasonable bar - and most enterprises are not yet there.

Does DORA apply to non-EU companies? ?

Yes. DORA applies to any ICT third-party provider serving EU financial institutions, regardless of where the provider is headquartered. Indian IT outsourcing firms, US cloud providers, and global managed security services companies all fall within scope if they serve EU-regulated financial entities. Non-compliance can result in penalties up to 2% of global annual turnover for critical third-party providers, plus potential loss of EU business.

2.4 Cloud Complexity & FinOps Pressure

The “cloud-at-any-cost” era is definitively over. The FinOps Foundation’s State of FinOps 2026 survey found that 98% of enterprises now manage AI spend as a core FinOps function - up from 31% just two years prior. Major cloud outages in 2025 - AWS US-EAST-1 (15+ hours), Google Cloud global authentication failure, and two Azure incidents - served as sharp reminders that cloud resilience requires deliberate architecture, not vendor trust.

Expert Insight

One of the most common mistakes I see in cloud architecture is the assumption that cloud-native means resilient. It does not. When AWS’s US-EAST-1 region went down for 15 hours in October 2025, it was not a failure of cloud technology - it was a failure of multi-region design in the organizations it disrupted. The enterprises that stayed operational had made deliberate architecture decisions upfront. The ones that scrambled had assumed the cloud would handle it.

KEY TAKEAWAY

Cloud resilience is an architecture decision, not a vendor promise. Enterprises must design for failure - multi-region, multi-cloud where justified - and validate that design through chaos engineering before an outage validates it for them.

03

BUSINESS RESILIENCY CHALLENGES

The following gaps represent the most pervasive issues observed across Global 2000 enterprise assessments. They are not technology failures. They are governance, process, and visibility failures that technology then exposes.

Operational & Process Gaps	Governance & Technology Gaps
Fragmented, siloed BCPs with no enterprise-wide view	Limited board-level visibility into resilience posture
Undefined or untested RTO & RPO targets	Technology sprawl - no single source of risk truth
Escalating ransomware & AI-powered supply-chain attacks	Talent gaps in crisis management & DR skills
Manual, slow incident response playbooks	No measurable resilience KRIs or KPIs
Cloud dependencies without adequate failover design	Regulatory mandates unmet: DORA, ISO 22301, RBI/SEBI
Backup strategies compromised by ransomware targeting	81% of material cyber incidents go unreported to leadership*
OT/IT convergence creating new attack surfaces	No AI-led detection or automated containment capability

* VikingCloud 2025 Cyber Threat Landscape Study

Expert Insight

The most dangerous gap I encounter is not the technology gap - it is the reporting gap. When 81% of material cyber incidents go unreported to leadership, it is not because CISOs are hiding information. It is because there is no agreed definition of what 'material' means, no escalation path that works under pressure, and often a cultural fear that disclosing an incident will be treated as a performance failure rather than an operational reality. Resilience starts with honest visibility - all the way to the board.

04

WHY BUSINESS RESILIENCE IS A BOARD-LEVEL PRIORITY

Resilience has historically been framed as a cost. The financial reality of 2025–2026 frames it as a return.

Cost of Inaction	Value of Investment
Average breach/outage cost: $4.44M (IBM, 2025)	3–8× ROI per $1 invested in structured resilience
Downtime up to $9,000/min for large enterprises	40–60% reduction in Mean-Time-to-Recover (MTTR)
Avg. ransomware recovery: 24 days of disruption	AI security teams resolve breaches 80 days faster (IBM, 2025)
Regulatory fines up to 4% of annual revenue (DORA)	AI use in security saves avg. $1.9M per breach (IBM, 2025)
Average breach/outage cost: $4.44M (IBM, 2025)	3–8× ROI per $1 invested in structured resilience
55% of CISOs faced attacks in 2025	Insurance premium reduction: 10–20%
23% customer churn without proactive resilience	Resilience as verified client & partner differentiator
$400B in annual global downtime losses	53% of orgs with tested backups recover within 1 week

Expert Insight

When I present the resilience ROI case to a board, I always start with the cost of one bad weekend - not a theoretical breach scenario, but a real outage number based on the organization's revenue profile. A $1 billion revenue company running 24/7 operations loses roughly $1.4 million for every hour of downtime. Once the board sees that number next to the cost of a structured resilience program, the conversation shifts from 'should we invest?' to 'what is the fastest path to capability?'

KEY TAKEAWAY

The board question is not 'can we afford to invest in resilience?' It is 'can we afford the cost of not investing?' The numbers have conclusively answered that question.

What is the ROI of investing in business resiliency?

?

Research consistently shows a 3–8× return on every dollar invested in structured business resilience, primarily through avoided downtime costs, reduced regulatory penalties, lower cyber insurance premiums (10–20% reduction), and faster incident recovery. organizations with AI-led security operations save an average of $1.9M per breach and resolve incidents 80 days faster than those without (IBM, 2025). Resilience investment also protects customer retention - proactive resilience programs have been linked to ~23% reduction in post-outage customer churn.

05

SERVICE OFFERINGS & CATALOGUE

Happiest Minds' AI-First, Agile-Always approach delivers a comprehensive, integrated resiliency capability across six service towers. AI-led tooling and automation fast-track every phase - from Discovery and Assessment through to full Implementation.

Service Tower	Key Offerings	Key Tools / Standards	Outcome
Platform Resiliency	Standardized landing zones, HA/DR design, SPOF elimination, multi-account architecture	AWS/Azure/GCP HA patterns, Terraform IaC, Chaos Engineering	Improved availability; consistent platform operations
Operational Resiliency	ITIL-driven service management, proactive monitoring, incident reduction, CSI	ServiceNow, PagerDuty, Dynatrace, AIOps platforms	Reduced MTTR; improved SLA adherence
Cyber Resiliency	CSPM, vulnerability management, SIEM/SOC integration, TLPT, Zero Trust alignment	CrowdStrike, Prisma Cloud, Sentinel, MITRE ATT&CK	Reduced risk exposure; improved security posture
Delivery & Engineering Resiliency	DevSecOps enablement (CI/CD, IaC), automation, platform engineering, release safety	GitHub Actions, Jenkins, ArgoCD, SonarQube	Faster deployments; reduced manual effort
Financial Resiliency (FinOps)	Cost visibility, rightsizing, AI spend governance, FinOps Framework v2.0 alignment	CloudHealth, Apptio, AWS Cost Explorer	20–30% cost optimisation; predictable spend
Governance & Reporting	KRI/KPI dashboards, regulatory compliance mapping, board-level reporting cadence	Power BI, Grafana, GRC platforms, DORA/ISO 22301 controls	Transparent resilience posture; audit confidence

Expert Insight

The most common mistake enterprises make when procuring resilience services is buying individual towers in isolation. Cyber Resiliency without Operational Resiliency means your detection is good but your response is slow. Platform Resiliency without Governance means you have failover capability that nobody has tested and nobody is accountable for. These six towers are designed to function as a system - each one reinforces the others.

SOLUTION APPROACH
THE 4E FRAMEWORK

Happiest Minds has developed the 4E Framework - a structured, AI-accelerated methodology that creates a living resilience program rather than a point-in-time project. Each phase builds directly on the last.

01

Explore

Risk & maturity baseline across people, process & technology; BIA initiation; stakeholder interviews; threat modelling; AI-led asset discovery

Typical Duration **3–6 weeks**

02

Envision

Target-state architecture; RTO/RPO definition & validation; control gap mapping; resilience blueprints; regulatory alignment (DORA, ISO 22301)

Typical Duration **4–6 weeks**

03

Engineer

Implement resilience controls; automate failover & runbooks; CI/CD hardening; chaos engineering; tabletop exercises; DR rehearsals with documented outcomes

Typical Duration **8-12 weeks**

04

Enhance

Continuous monitoring; KRI/KPI dashboards; governance cadence; board-level reporting; iterative improvement based on incident learnings

Typical Duration **Ongoing**

Expert Insight

The 4E Framework was designed to solve a problem I kept encountering in large engagements: organizations would complete an assessment, receive a gap report, and then do nothing with it because the path from 'where we are' to 'where we need to be' felt overwhelming. The framework breaks that journey into phases with clear outputs at each stage - so there is always a tangible deliverable, always a board-presentable artefact, and always a defined next step. Resilience becomes a continuous operating discipline, not a one-time project.

The 4E Framework is AI-accelerated: automated discovery tools reduce assessment time by up to 60%, while AI-driven runbook generation and chaos experiment design eliminate months of manual effort from the Engineer phase.

How long does a business resiliency assessment take?

?

With AI-accelerated tooling, a comprehensive enterprise resilience assessment covering all five resiliency towers (Cyber, Platform, Operational, Delivery, and FinOps) can be completed in 3–6 weeks. This includes maturity scoring, gap analysis, regulatory alignment (DORA, ISO 22301), and a board-ready roadmap. Traditional manual approaches take 8–12 weeks for comparable coverage. The Happiest Minds 4E Framework's Explore phase typically delivers a scored baseline and prioritized recommendations within this 3–6 week window.

07

MATURITY FRAMEWORK & ASSESSMENT MODEL

Happiest Minds' AI-led maturity framework evaluates the enterprise IT environment across five resiliency towers, producing a scored (0–5) maturity report with a prioritized, time-bound roadmap aligned to ISO 22301, NIST CSF, DORA, and the CMMI model.

Maturity Level	Cyber Resiliency	Platform & Infra	Operational	Delivery & Eng.	Financial (FinOps)
Current Benchmark	2.5	2.4	2.3	2.4	2.2
Level 5 – Optimized	Predictive resilience; continuous AI validation; self-healing	Self-healing platforms; resilience by design; automated failover	Autonomous ops; predictive prevention; zero-touch remediation	Intelligent pipelines; continuous delivery optimization	AI-driven spend governance; 98% AI spend managed
Level 4 – Quantitative	Risk & recovery measured; evidence-based closure	Resiliency KPIs tracked; recovery predictability	MTTR & automation metrics tracked	Pipeline reliability & flow metrics measured	Spend predictability; optimization ROI tracked
Level 3 – Defined	Risk-aligned controls; DR integrated; DORA-aligned	Standardized IaC; DR tested; AZ survivability validated	Defined SLOs; structured incident/change management	Standardized pipelines; DevSecOps embedded	Cost forecasting; backlog-driven optimisation
Level 2 – Managed	Core controls & governance; basic SIEM	Basic redundancy for critical infra	Centralized ops; basic automation	Standard tools; basic DevSecOps	Cost tracking; basic tagging
Level 1 – Reactive	Ad-hoc security; limited visibility	Minimal redundancy; unmanaged infra	Firefighting; manual incident handling	Ad-hoc CI/CD; manual releases	No cost control; no ownership

Expert Insight

The maturity model is not designed to tell organizations they are failing. It is designed to tell them precisely where they are and what the next step looks like. The most common reaction when I present a Level 2 score is relief - because for the first time, the CISO has a language to explain to the board why resilience investment is needed, and a map of where that investment should go. A number is actionable. A narrative is not.

What is a business resiliency maturity model?

?

A business resiliency maturity model is a structured framework that scores an organization's resilience capability across defined dimensions - typically cyber, platform, operational, delivery, and financial - on a scale from Level 1 (Reactive) to Level 5 (Optimized/AI-Driven). The model identifies current-state gaps, benchmarks performance against industry peers, and produces a prioritized roadmap for improvement. Happiest Minds' maturity assessment, aligned to ISO 22301, NIST CSF, and DORA, delivers a complete scored report and board-ready roadmap in 3–4 weeks.

08

INDUSTRY-SPECIFIC RESILIENCY CONSIDERATIONS

Resiliency requirements vary significantly by sector. The following reflects Happiest Minds' cross-industry delivery experience across Global 2000 organizations.

Industry	Primary Threat Vectors	Regulatory Obligations	Priority Controls
Financial Services	Ransomware, API fraud, insider threats, supply-chain ICT risk	DORA (Jan 2025), RBI/SEBI, PCI DSS, ISO 22301	TLPT, third-party ICT risk registers, real-time incident reporting
Healthcare & Life Sciences	Ransomware (avg. $7.42M breach), OT/medical device attacks, data exfiltration	HIPAA, GDPR, local health data regulations	OT/IT segmentation, tested backup & recovery, CSPM, BIA refresh
Manufacturing & Supply Chain	OT/SCADA attacks, MSP-targeting, production halts	NIST CSF, ISO 27001, CISA sector guidelines	ICS/OT resilience, DR for production systems, supply-chain risk profiling
Technology & SaaS	Cloud misconfiguration, third-party dependency risk, CI/CD pipeline attacks	SOC 2 Type II, ISO 27001, GDPR	Secure CI/CD, chaos engineering, multi-region failover, FinOps governance
Retail & E-Commerce	Peak-load failures, payment fraud, DDoS, data breaches	PCI DSS, GDPR, consumer protection laws	HA/DR for commerce platforms, DDoS mitigation, FinOps cost controls

Expert Insight

Healthcare is the sector that keeps me up at night. The average breach cost is $7.42 million - the highest of any industry - but the real stakes are not financial. They are clinical. When a hospital's systems go down, the question is not when you will restore data. It is whether a patient in the ICU will receive the right medication while you restore it. That is why OT/IT segmentation and validated offline backup procedures are non-negotiable in healthcare - they are not compliance requirements; they are patient safety requirements.

What are the biggest cybersecurity risks in the healthcare industry in 2026?

?

Healthcare faces the highest breach costs of any industry at $7.42M average per incident. The primary threats in 2026 are ransomware targeting electronic health record systems, attacks on connected medical devices and OT infrastructure, and data exfiltration of patient records for sale on dark web marketplaces. Regulatory obligations under HIPAA and GDPR add further exposure. Priority controls include OT/IT network segmentation, immutable and tested backup systems, CSPM for cloud-hosted clinical systems, and regular BIA refresh to account for new medical technology dependencies.

09

REGULATORY LANDSCAPE: DORA, ISO 22301 & BEYOND

DORA (Regulation EU 2022/2554) establishes unified ICT risk management requirements across all EU financial entities and their technology providers. In 2026, regulators are no longer reviewing readiness assessments - they are demanding live operational proof.

1

ICT Risk Management

Comprehensive frameworks for identifying, protecting, detecting, and recovering from ICT disruptions (Article 11: operational continuity mandate).

2

Incident Reporting

Major ICT incidents must be reported to competent authorities within defined timeframes. Structured notification: initial, intermediate, and final report (Articles 17–18).

3

Resilience Testing

Advanced Threat-Led Penetration Testing (TLPT) required for significant financial entities; regular DR testing for all in scope.

4

Third-Party Risk Management

Rigorous oversight of ICT providers (Articles 28–31). In November 2025, ESAs designated 19 Critical ICT Third-Party Providers including AWS, Google Cloud, Microsoft, Oracle, and SAP.

5

Information Sharing

Collaborative threat intelligence sharing between financial entities and competent authorities (Articles 24–27).

Non-EU technology providers serving EU financial institutions must comply with DORA. Many Indian IT outsourcing and global managed services firms are now in scope. In 2026, regulators are conducting active enforcement reviews - not just accepting policy documentation.

Other Key Frameworks

Framework	Scope	Key Enterprise Requirement
ISO 22301:2019	Global - Business Continuity Management	BCMS certification; documented BIA, RTO/RPO, tested continuity plans
NIST CSF 2.0	Global - Cybersecurity Framework	Govern, Identify, Protect, Detect, Respond, Recover functions
RBI / SEBI (India)	Indian financial institutions	IT Risk & Cyber Security Framework; DR mandates; audit trails
RBI / SEBI (India)	Indian financial institutions	IT Risk & Cyber Security Framework; DR mandates; audit trails
HIPAA Security Rule (US)	US Healthcare	Risk analysis, contingency plan, disaster recovery procedures
NIS2 Directive (EU)	Critical infrastructure sectors	Incident reporting, supply-chain security, executive accountability

Expert Insight

The organizations that are most exposed to DORA enforcement in 2026 are not the ones that ignored it. They are the ones that completed a gap assessment in 2024, documented their frameworks, and then assumed the job was done. DORA's 2026 enforcement phase is specifically looking for operational evidence - incident logs, DR test reports, vendor oversight records, and real-time control dashboards. A well-written policy without operational proof is, in regulatory terms, the same as no policy.

What does DORA compliance require in 2026?

?

In 2026, DORA compliance requires operational evidence - not just documented frameworks. Regulators expect live ICT risk management dashboards, completed TLPT exercises, structured incident reporting within defined timeframes, a maintained Register of Information for ICT third-party providers, and tested DR procedures. The 2026 enforcement environment has moved from 'show us your policies' to 'show us your resilience in practice.' organizations must also manage concentration risk arising from Critical Third-Party Providers (CTPPs) designated by the ESAs in November 2025.

10

BUSINESS BENEFITS

These benefits are drawn from Happiest Minds' delivery experience with Fortune 2000 customers across financial services, manufacturing, healthcare, technology, and retail sectors.

Financial

Business Benefit
Reduce unplanned downtime costs and regulatory penalties; protect revenue

Avg. $1.9M saved per breach with AI-led security (IBM, 2025)

Operational

Business Benefit
Faster incident recovery with RTO/RPO met; significantly reduced MTTR

40–60% MTTR reduction; **53%** recover within 1 week (Sophos, 2025)

Reputation

Business Benefit
Maintain customer trust; protect brand equity during disruption events

~23% customer churn avoided post-outage

Regulatory

Business Benefit
Continuous compliance with DORA, ISO 22301, NIST CSF, SEBI/RBI

Audit confidence; regulatory safe harbour

Strategic

Business Benefit
Resilience as competitive differentiator; unlock new market opportunities

3–8× ROI per $1 invested

Financial (FinOps)

Business Benefit
Cloud cost visibility, rightsizing, AI spend governance

20–30% cloud cost optimisation

Workforce

Business Benefit
Employee confidence & productivity through defined crisis playbooks

Reduced decision paralysis; faster coordinated response

Insurance

Business Benefit
Demonstrable resilience controls reduce cyber insurance premiums

10–20% premium reduction

STRATEGIC VALUE

Happiest Minds Technologies is uniquely positioned as an AI-First, Agile-Always enterprise technology partner. Our resiliency practice combines deep domain expertise with AI-led tooling to deliver measurable outcomes - not technology implementations in search of a business case.

AI-led digital engineering
Predictive resilience that moves beyond reactive response, spanning product engineering, infrastructure, cybersecurity, analytics, automation, and GenAI.

AI-accelerated assessment
Reducing maturity assessment timelines by up to 60%, delivering board-ready gap analysis and roadmaps in 3–4 weeks.

Secure-by-design delivery
For regulated, mission-critical, and globally distributed environments, including DORA-aligned frameworks for EU financial entities.

Cross-industry experience
Serving Fortune 2000 enterprises across BFSI, healthcare, manufacturing, technology, and retail with sector-specific accelerators and playbooks.

Platform thinking
Across hybrid cloud, data, digital products, integration, and AI orchestration, with FinOps governance ensuring cost and performance accountability at scale.

Outcome-led execution
Every engagement is benchmarked against measurable resilience KRIs/KPIs, not technology delivery milestones.

Expert Insight

The question I am most frequently asked by CXOs is: 'How do I know our resilience program is actually working?' My answer is always the same: if you cannot answer three questions - What is your current RTO/RPO? When did you last test it? What did the test reveal? - then your program is theoretical, not operational. The work we do at Happiest Minds is designed to make those three questions answerable at any board meeting, on any given day.

RECOMMENDED NEXT STEPS

The path to enterprise resilience is a structured journey, not a one-time project. This roadmap is designed for organizations at Maturity Level 2–3 seeking to systematically close gaps and build a board-visible, AI-enabled resilience capability.

Horizon	Scope	Key Enterprise Requirement
Immediate (2–4 Weeks)	Conduct Executive Resilience Workshop & current-state assessment using the Happiest Minds 4E maturity model	Scored maturity report across 5 towers; executive briefing pack
Short-term (1–3 Months)	Deliver Business Impact Analysis (BIA), prioritized risk register, and DORA/ISO 22301 gap assessment	Risk register; control gap report; regulatory compliance roadmap
Mid-term (3–6 Months)	Implement top 3 resilience controls; automate incident runbooks; run first DR simulation with documented outcomes	Hardened controls; validated RTO/RPO; DR test report for audit
Mid-term (6–9 Months)	Establish FinOps governance; deploy KRI dashboards; integrate SIEM/SOC with automated response playbooks	Cost optimisation baseline; live KRI dashboard; SOC integration
Ongoing (9–12+ Months)	Establish resilience governance board; quarterly board-level KRI reporting; continuous chaos engineering cadence	Board-ready resilience scorecard; continuous improvement program

ABOUT THE AUTHOR

Rambabu Pothu
Global Consulting & Implementation Head, IMSS

Rambabu Pothu is the Global Consulting & Implementation Head for the Infrastructure Management & Security Services (IMSS) practice at Happiest Minds Technologies. With over two decades of experience in IT infrastructure, consulting, and global program delivery, Rambabu leads a cross-geography practice spanning the USA, UK, India, Middle East, Australia, and New Zealand. He has built specialized teams in Enterprise Business Resiliency, DORA-aligned ICT Risk Management, Cloud & Platform Architecture, and AI-led Security Operations.

For further insights, assessments, or to request a CXO briefing, write to us at **business@happiestminds.com**

ABOUT HAPPIEST MINDS

Happiest Minds Technologies Limited (BSE, NSE: HAPPSTMNDS) is an AI First, customer-centric digital engineering company committed to delivering 'Happiest People . Happiest Customers'. With an integrated approach that spans from chip to cloud, Happiest Minds delivers secure and scalable solutions across product engineering, cybersecurity, analytics , and automation platforms. Happiest Minds brings purpose and precision to every engagement, helping enterprises solve complex business challenges and fast-track their digital evolution across industry sectors such as Banking, Financial Services & Insurance (BFSI), EdTech, Healthcare & Life Sciences, Hi-Tech and Media & Entertainment, Industrial, Manufacturing, Energy & Utilities, and Retail, CPG & Logistics.

Happiest Minds has been honored by both the Golden Peacock Awards and the Institute of Company Secretaries of India (ICSI) for its exemplary Corporate Governance practices. Guided by its mission of 'Happiest People . Happiest Customers' and consistently recognized as a great place to work, Happiest Minds is headquartered in Bengaluru, India, with a global presence across the Americas, UK, Europe, Australia, the Middle East, Africa, and Asia.

happiest minds
AI FIRST. AGILE ALWAYS.