



Embedding resilience

Becoming cyber resilient through accepting the threat

42%

of organisations reported phishing and social engineering attacks in 2024¹

90%

of organisations expect an increase in cyberattacks this year in terms of volume, costliness, or both²

29%

of organisations reported that they had been materially affected by a cyber incident in the past 12 months³

Cybercrime is predicted to cost the world about €10.5 trillion in 2025, according to Cybersecurity Ventures. If it were measured as a country, then cybercrime would be the world's third-largest economy after the U.S. and China.⁴

Cybercrime, often called the dark underbelly of digitalisation, continues to rise rapidly like an epidemic. While organisations are inclined to focus on prevention, the alarming statistics should push us to accept the reality that attacks are inevitable and adopt the “when, not if” approach, shifting our pursuit from the illusion of perfect security toward an achievable goal of cyber resilience.

There is much industry discussion regarding the transition from reactive to proactive cybersecurity, but true cyber resilience demands both. We must accept the inevitable: our organisations will be attacked. While detection and prevention remain crucial, the hallmark of a resilient organisation lies in its ability to respond to and recover from cyber incidents effectively. This mindset means putting measures in place that limit damage and keep critical functions running—ensuring your business stays operational even against the most sophisticated attacks.

This resilience-focused approach becomes even more critical as digital transformation accelerates, exponentially expanding the threat surface. When treated as a strategic enabler rather than a constraint, cyber resilience—embedded throughout the organisation’s operating model—can actually amplify digital initiatives while digital capabilities strengthen security postures. Organisations must, therefore, integrate robust security controls into all transformation projects (including new product launches, acquisitions, and market expansions) from inception, not as an afterthought. Cyber resilience transcends being merely an incident-driven technical function; it is a dynamic mindset and adaptive culture that evolves alongside both threats and opportunities.

While tools like firewalls and threat detection systems play an essential role, true resilience depends on people, processes, and leadership commitment to cybersecurity best practices. A resilient culture means that employees at all levels understand cyber risks, take proactive measures, and respond effectively to incidents—not just the IT team. Much like digitalisation and customer-centricity have evolved from isolated initiatives to organisation-wide imperatives, cybersecurity must follow the same path to maturity. This evolution involves continuous training, clear communication, and integrating cybersecurity into business decisions rather than treating it as a separate technical concern. Ultimately, cyber resilience thrives when security becomes a shared responsibility embedded into daily operations and decision-making across an organisation.

¹ <https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/>

² <https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2>

³ <https://www.weforum.org/publications/global-cybersecurity-outlook-2024/>

⁴ <https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger>



The importance of continuous and iterative cybersecurity: The WannaCry cyberattack

On May 12, 2017, the world witnessed one of the gravest ransomware attacks in history—WannaCry. This self-propagating ransomware worm exploited a vulnerability in Microsoft Windows called EternalBlue, a leaked exploit allegedly developed by the U.S. National Security Agency (NSA). The attack spread rapidly across the globe, encrypting files on infected systems and demanding \$300 in Bitcoin for decryption, doubling if payment wasn't made within three days.

Within hours, WannaCry had infected more than **230,000 computers in 150 countries**. Hospitals, banks, telecom companies, and government agencies were among the hardest hit. The UK's National Health Service (NHS) suffered massive disruptions with up to 70,000 affected devices, from MRI scanners to operating theatres, forcing hospitals to cancel surgeries and turn away patients. FedEx, Boeing, Deutsche Bahn, and many automotive manufacturers were also affected.

Organisations faced severe consequences: financial losses, operational disruptions, and reputational damage. **The global cost is estimated at between €4 and €8 billion.**

Despite its scale, WannaCry could have been prevented. Microsoft had released a security patch (MS17-010) two months prior, but many organisations, for one reason or another, had yet to update their systems. Beyond patching, a comprehensive resilience approach—including initiatives such as proper governance, network segmentation, endpoint detection, backup strategies, incident response planning, and employee awareness—would have significantly reduced the impact.

A major turning point came when a security researcher, Marcus Hutchins, accidentally discovered a ‘kill switch,’ a hardcoded domain that, when registered, stopped WannaCry’s spread. While this fortunate discovery helped contain the initial outbreak, variants without this kill switch later emerged. This evolution demonstrates that reliance on reactive, one-time solutions is inherently risky. Had organisations implemented a culture of resilience rather than depending on emergency interventions, they would have been better positioned against both the original attack and its variants.

The WannaCry saga ultimately proves that cyber resilience requires systematic, proactive approaches rather than hoping for last-minute rescues.



Resilience is a sign of maturity in an organisation. Robust organisations have pivoted from the misguided notion of outright prevention to a focus on resilience—the “when, not if” mentality. Those same organisations understand that a high wall is never enough; a plan must be developed, implemented, and tested for when an organisation is breached, but a real plan, not just a token one.

Token efforts vs. business benefit

Despite the clear risk, many, if not most, companies are not acting with sincerity in the face of growing cyberattacks. Token efforts are the norm. There are two key indicators of such superficial approaches: First, companies that lack a senior business leader who champions cybersecurity at the executive level. While formal structures may vary, the absence of C-suite advocacy and accountability—whether through a dedicated information security board or direct representation in leadership meetings—signals that security isn't truly embedded in business strategy. The second indicator is inadequate risk management: either cyber risks are absent from operational risk registers entirely, or they exist merely as generic entries without proper classification, regular updates, or specific mitigation plans. Simply having “cyber” listed on a risk register without corresponding awareness campaigns and training for all employees reveals a disconnect between acknowledged risks and meaningful action.

To some extent, this is understandable; the market demands we “move fast,” forcing us into a constant race to deliver products and services quickly. This urgency often relegates security to secondary importance due to the misconception that it impedes speed and agility. When security isn’t integrated from the beginning as part of the design process, it becomes a bottleneck, requiring expensive rework and retroactive changes. What’s ironic is that secure-by-design products actually serve as powerful market differentiators in today’s landscape, where consumers increasingly value the protection of their data and privacy.

Take AI, for example. If a proven-secure AI product existed, that would be a market differentiator. Imagine a self-driving car with engineered resilience in data protection and also in servicing the vehicle and in customer relationships. But this does not exist.

The era of “tech” businesses and “non-tech” businesses has passed. When everyone and everything is connected to the internet, everyone and everything has an attack vector. So, everything today is a tech business, making data breaches a business problem, not a technology issue. Yet this view has not yet been universally accepted in organisational cultures, and cyber resilience is often the victim of budget restraints and/or cuts. Given the difficulty of demonstrating true value and ROI regarding cyber resilience and security, it is still too often seen as a tradeable commodity, a hindrance instead of an enabler. But it does not have to be this way.



Business benefit defined

Quantifying the ROI on an investment in cyber resilience is challenging but not impossible. While traditional financial metrics may struggle to capture the full value of resilience measures, organisations can develop meaningful frameworks to assess both direct and indirect returns. This is especially true as the business value of cyber resilience extends beyond simply avoiding costs, encompassing regulatory compliance, operational continuity, and stakeholder trust, all of which contribute to measurable outcomes when adequately evaluated. With the right approach, cyber investments can demonstrate clear value, even if that value takes multiple forms.

Take, for example, the European Union’s Cyber Resilience Act. While the CRA is not applicable in the United States or the United Kingdom, these countries have, or soon will, their own fundamentally similar¹ legislation—a mandated cyber resilience requirement to do business within their territory. So, one quantifiable return on cyber resilience is the very ability to operate in those markets.

A second quantifiable benefit is reduced spending on incident response and recovery. For example, in 2024, the average cost of a data breach was €4.66 million, and the average cost of a malicious insider attack was €4.76 million, according to IBM’s Cost of Data Breach Report.



¹ <https://www.lexology.com/library/detail.aspx?g=12363882-4860-4e64-944c-3c5be3e327ab>

Average cost
of a data breach in 2024 was

**€4.66
million**

Average cost
of a malicious insider attack in 2024 was

**€4.76
million**

However, Accenture's research shows that those who prioritize cyber investments experience up to three times lower cyber breach costs than their peers.

So, a security program as a resilience measure is an order of magnitude cheaper than trying to rebuild the company post-compromise. This is true both financially and reputationally, the latter more often reflected in customer behaviour or share price.

Take, for example, the shipping giant Maersk—the NotPetya ransomware attack in 2017 infected almost 50,000 of their systems across 600 sites in 130 countries. The losses grew to nearly €300 million, affecting close to 90,000 workers, port infrastructure, customers, and end-users. This single attack caused a 20% drop in business volume.

Within the public sector, cyber incidents can also cause serious downtime, disrupting essential services and threatening public safety and national security.

Finally, it is worth noting that companies that respond well to a cyberattack—meaning they have resilience measures in place and react with speed and transparency—typically experience stronger recoveries, often seeing their share prices rise above pre-incident levels. The Accenture State of Cybersecurity Resilience 2023 emphasizes this, terming companies that align security with business objectives “cyber transformers.” These companies reported 26% lower costs from breaches than other respondent organisations and were 18% more likely to increase revenue growth.

Effective incident response and transparent communication significantly impact reputation—particularly crucial for public sector organisations where reputation directly builds citizen trust, an asset more valuable than gold. Trust serves as democracy's foundation, providing governments with the legitimacy needed for effective operation. Citizens willingly share their data in trusted relationships, enabling enhanced digital services. However, this creates an obligation for organisations to safeguard the data entrusted to them. At Nortal, we define trust through the principles of reliability, fairness, and transparency, with successful execution being the critical factor that brings these elements together.¹

Nortal trust formula:

Trust = reliability x fairness x transparency ± execution

¹ <https://nortal.com/insights/creating-trust-digital-government/>

The cost of resilience

So, what does cyber resilience cost? It is not a percentage of your turnover but rather depends on your needs.

The key questions to ask are:

- How does the organisation make money or deliver value?
- What are the organisation's critical outputs and/or services provided?
- What is the threat to each?
- Does it matter if these systems or information are unavailable for an hour? A day? A week? Can the business continue to function?
- Ultimately, what compensating or mitigating controls need to be put in place?



The answers to these questions dictate the resilience measures needed and, thus, costs. The most important aspect is that the cyber resilience program is aligned with the business. It is a mistake to optimise for the wrong problem. A company that does not manufacture nuclear missiles may not need state-of-the-art security; for a local bakery, state-of-the-art would arguably be overkill. High levels of resilience are expensive and might be unnecessary for your business context. But if you operate a real-time business, having your services unavailable even for a few seconds or minutes could mean more revenue lost than a solution would cost.

The human element represents a significant cost factor in cyber resilience planning. According to Verizon's 2024 Data Breach Investigations Report¹, 68% of breaches involve a non-malicious human element, making people the most expensive vulnerability to address. Social engineering attacks succeed when employees click malicious links or divulge sensitive information, often resulting in costly breaches.

Failing to invest in human-centred resilience measures represents a substantial financial risk. A comprehensive cyber resilience budget must allocate resources to inform and train employees, conduct regular security exercises to test defences, and develop robust response and recovery protocols. The cost extends beyond internal measures to include communication systems for stakeholders, customers, and regulatory bodies. This human dimension of cyber resilience is a discipline requiring specific investment but one that typically delivers the highest return in breach prevention and cost avoidance.

Most important is to realize there is no "silver bullet." The fact that millions are spent is no guarantee of security. True cyber resilience means a constant review of investment to keep pace with changing threats and adversaries. One does not build a house in a dangerous neighbourhood without expecting to incur security expenses. Thieves are constantly finding new ways of breaking and entering, and the market keeps pace with the development of better locks and alarms. For this reason, cyber resilience should be viewed as a continuous process that must be sized to the needs of the business.



¹ <https://www.verizon.com/business/resources/reports/dbir/>

The building blocks of embedding resilience

A complete checklist to a comprehensively cyber resilient organisation

B1 Governance & strategy

The “why” of cyber resilience sets the vision, policies, risk appetite, risk tolerance, and strategic direction.

A comprehensive governance and strategy framework is at the heart of any cyber resilience program. This building block functions as the command centre of cyber resilience, setting the overarching vision, establishing critical policies, and defining the organisation’s risk appetite alongside its strategic direction. Meticulously mapping internal policies to the requirements of various external frameworks creates a resilient and compliant operational environment.

- Leadership commitment and clear accountability
- Risk management and asset identification (aligns with NIST’s Identify function and ISO’s context and leadership clauses)
- Integration of cyber resilience into business continuity planning
- Regular review and refinement of policies to address evolving threats
- Regulatory and legal compliance, mapping to relevant standards
- Organisational value alignment; cyber strategies support business objectives and value generation
- Reporting structures and escalation pathways
- Investment prioritization
- Operational dependency mapping
- Operational Impact analysis (BIA)

B2 Protect & secure

The traditional defence layer implements technical and procedural safeguards to minimise the likelihood of breaches.

Having all the technical and procedural safeguards in place helps maintain a vigilant stance and enhances the continuous monitoring of the security posture. In essence, while the protect and secure element aims to prevent incidents through a layered defence approach, it is also a critical foundation that supports the other building blocks of cyber resilience.

- Deliberate security architectures aligned to organisational goals, objectives, and structures
- Resilience by design principles
- Supply chain security controls
- Security culture and capability development
- Access controls, encryption, and network security measures
- Endpoint and application security
- Regular vulnerability assessments, patch management, and continuous security and business alignment validation
- Alignment with the “Protect” function of NIST and the Annex A controls of ISO 27001

B3 Resilient response & business continuity

Ensures the organisation can effectively respond to incidents while maintaining critical business operations, minimising impact, and returning to normal functioning.

Acknowledging that no security posture is impervious to all threats, this building block integrates incident response capabilities with business continuity planning. This integrated approach is particularly distinctive in that it assumes incidents are inevitable and thus focuses on both swift tactical response and sustained operational resilience. By combining these elements, organisations can minimise downtime, maintain service delivery, and preserve customer trust throughout the incident lifecycle.

- Incident response planning and crisis management frameworks
- Business continuity strategies aligned with organisational priorities
- Cross-functional coordination with clearly defined roles and responsibilities
- Real-time damage assessment tied to operational impact metrics
- Predefined operational priorities to guide resource allocation during incidents
- Alternative processing capabilities for critical business functions
- Systematic restoration procedures following predetermined sequence priorities
- Stakeholder communication protocols scaled by incident severity
- Redundancy in systems and data processing capabilities
- Service Level Resilience Objectives that balance security and operational requirements
- Supply chain security and third-party risk management
- Simulated exercises and tabletop drills to validate response and continuity measures
- Processes for rapid containment and eradication of threats
- Operational dependency mapping to identify critical business pathways
- Post-incident reviews to assess effectiveness and identify improvements

B4 Intelligence & adaption

A continuous learning loop that leverages threat intelligence, real-time monitoring, and post-incident analysis to evolve defences and responses

The intelligence and adaption block ensures that organisations can systematically analyse the value of their current defences and make informed adjustments where necessary. Moreover, the adaption process involves internalizing lessons learned from post-incident reviews and active engagement with external intelligence sources and collaborative industry networks. This ensures that our organisations learn and grow from our own experiences and also from those of other organisations. It also ensures that we remain at the forefront of best practices and can continually refine our policies and processes to meet new challenges head-on.

- Proactive threat hunting and continuous monitoring
- Intelligence-led testing and validation
- Analytics, reporting, and feedback mechanisms
- Emerging Tech impact assessments
- Predictive analytics
- Incorporation of lessons learned into strategy, policy, and process updates
- Engagement with external intelligence sources and collaboration with industry peers
- Review of emerging threats and recommendations regarding strategy, policy, and process



Embedding resilience

To embed the cyber resilience process, we need to embrace erudition, constantly learn from our mistakes, and then adapt and apply those lessons to any given context, not once, not twice, but continuously. Cyber resilience can then be embedded through four distinct phases, constantly monitored as threats and risks evolve.

Approaches to embedding cyber resilience will necessarily vary based on organisational maturity. Organisations with lower maturity levels should prioritize foundational understanding—identifying problems, mapping threats, and quantifying the business impact of potential downtime or data loss. Meanwhile, more mature organisations can devote greater resources toward implementation and advanced resilience strategies, building upon their existing security framework.

Phase 1: Mission mapping

Mission mapping begins with a deep exploration of organisational purpose, going beyond surface-level statements to understand the fundamental value an organisation provides to its stakeholders. This understanding forms the basis for identifying critical functions—those essential activities that must be maintained even under adverse conditions.

Value stream and dependency mapping provide insight into how the organisation creates and delivers value, revealing obvious and subtle interdependencies that could affect resilience. This mapping exercise extends to stakeholder relationships, creating a comprehensive understanding of how the organisation interacts with its ecosystem, including its supply chain.

This phase is the key element to resilience. Knowing an organisation's purpose and how it fulfils that purpose allows assumptions to be made and examined. Take an electric vehicle company as an example. One might assume the company earns its revenue from selling vehicles, which may be true. But what if it made its revenue from reselling data to other manufacturers of vehicles? Incorrect assumptions often lead to over-optimisation for the wrong outcome. Historically, this problem has been made worse as cyber was seen as a technical problem, one decoupled from the business context and given to engineers to resolve. Present an engineer with a problem, and it's possible you'll receive an exquisite overengineered solution. Mission mapping ensures that the right business problem is addressed so that solutions are scaled and applied where they are actually needed.

Phase 2: Capability assessment

Capability assessment involves systematically evaluating an organisation's current adaptive capacity (its ability to absorb disruption without critically impacting business operations and/or value generation), therefore, gauging its ability to respond to both challenges and opportunities. This assessment spans protection security measures, operational flexibility, and intelligence capabilities, providing a comprehensive view of organisational resilience.

The assessment process employs both quantitative (recovery time objective (RTO), Mean Time to Detect (MTTD), and qualitative (Resilience Culture Assessment, Crisis Simulation Performance) measures, recognizing that resilience cannot be reduced to simple metrics. Instead, it considers multiple capability dimensions, from technical controls to human factors and organisational culture.

Phase 3: Gap analysis

Gap analysis compares an organisation's current resilience posture against its desired state, identifying areas for improvement across all framework layers. This desired state is typically defined through industry frameworks (such as NIST Cybersecurity Framework, ISO 27001, etc.), regulatory requirements, and organisation-specific objectives established during the mission mapping phase. This analysis considers not just capability gaps but also opportunities for enhancement and innovation.

The prioritization of improvements considers both the criticality of identified gaps and the organisation's capacity for change (an element of its adaptive capacity). Action planning then creates realistic roadmaps for closing these gaps while maintaining operational stability and acknowledging constraints (time, budget, etc.).

Phase 4: Implementation

Implementation focuses on executing prioritized improvements while maintaining operational continuity. This phase emphasizes incremental improvement, balance across technology and culture, and the importance of measurement and feedback. It ensures that improvements achieve their intended outcomes while avoiding unintended consequences and/or seizing fleeting opportunities.

Establishing feedback mechanisms and learning protocols ensures that the implementation process contributes to organisational learning and capability development (value generation). This creates a virtuous cycle that can fundamentally alter the business, requiring a re-evaluation of mission mapping and continuous improvement in resilience capability.

Conclusion

Adopting the “when, not if” mindset ensures that organisations are prepared to detect, respond to, and recover from cyber threats with minimal disruption. Resilience is not a one-time investment but an ongoing commitment—requiring continuous monitoring, training, and adaptation to remain effective. By embedding cyber resilience into daily operations and long-term planning, organisations can mitigate damage, maintain trust, safeguard business continuity, and save money. In an era where cyber threats are inevitable, true resilience lies in a culture of resilience-by-design thinking.





Get in touch

Nortal offers a national defence-level pedigree in building cyber-resilient organisations. Get in touch to detect, prevent, respond to, and recover from cyber incidents.

About the authors

Michael Hampson, a leading cybersecurity expert in the UK, with a career spanning over 25 years and a long history in the defence industry, including the UK's Ministry of Defence.

James Thomas, Global Head of Cyber at Nortal.

Awarded a Royal commendation for his work in Cybersecurity, James spent 21 years in the UK military as a commander and leader in the Telecommunications, Cyber and Electronic Warfare branch of the British Army.

Contact: James.Thomas@nortal.com

nortal.com

25
years of shaping
the future