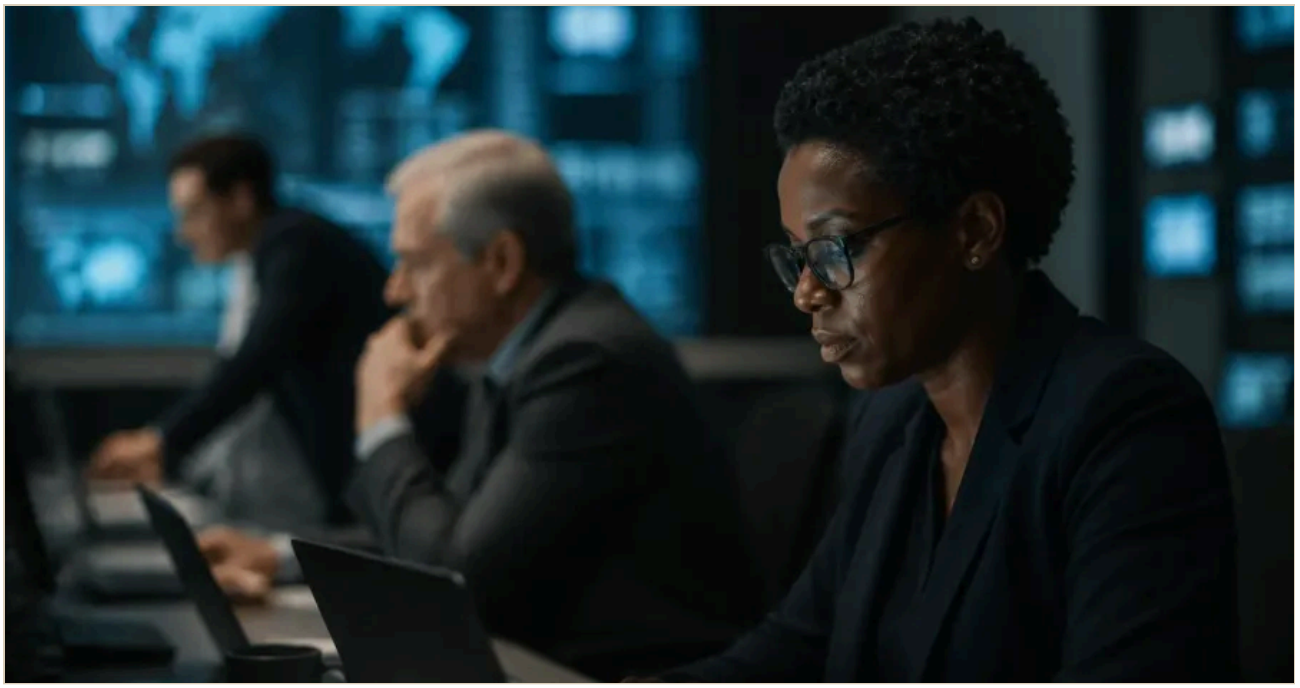

INTERNATIONAL RESEARCH INSTITUTE — FLAGSHIP REPORT

Cybersecurity and Digital Resilience for Public and Private Institutions

Cybersecurity · 2025-11-13 · Licence CC BY 4.0

Overview

For two decades, institutional cybersecurity was framed as a problem of prevention: build a strong enough perimeter, and intruders stay out. That framing has quietly collapsed. The combination of cloud migration, remote work, dense third-party dependencies and professionalised criminal and state-linked adversaries means that most large organisations should now assume compromise is a recurring condition rather than an exceptional event. The strategic question has moved from *how do we keep attackers out* to *how quickly can we detect, contain, and recover while continuing to operate*. This report treats that shift — from defence to resilience — as the central story of the sector, and assesses what it means for spending, market structure, regulation and public policy through 2030.

The market that has grown up around this problem is large and still expanding, but it is not the whole picture. We estimate global spending on cybersecurity products and services at roughly USD 190–220 billion in 2024, growing at a low-double-digit annual rate. Yet the losses the market is meant to contain — business interruption, extortion payments, remediation, regulatory penalty and reputational damage — are plausibly several times larger and far harder to measure. The gap between what is spent on protection and what is lost to incidents is the economic engine of the sector, and it explains why security has become a board-level and, increasingly, a sovereign concern rather than a technical line item.

The sector in brief

INDICATOR	VALUE
Global cybersecurity spending, 2024 — products & services; estimate	USD 190–220bn
Estimated market CAGR to 2030 — low double digits	~10–12%
North America share of global spend — directional estimate	40–45%
Global cyber workforce shortfall (roles) — structural constraint	Millions

Three forces now shape institutional behaviour more than the threat landscape itself. The first is regulation: a wave of binding rules in the European Union, United States and elsewhere is converting cybersecurity from a discretionary investment into a compliance obligation with personal and corporate liability attached. The second is concentration: a small number of cloud, identity and endpoint platforms increasingly underpin the digital economy, which raises the security floor for everyone but also creates correlated failure risk that individual buyers cannot diversify away. The third is automation on both sides of the contest, as artificial intelligence changes the economics of attack and defence simultaneously.

Our central judgement is that the sector is maturing into a managed, regulated, and consolidated market — closer to how safety and financial risk are handled than to a frontier technology race. That maturation is broadly stabilising, but it carries two under-priced tail risks: a systemic outage or compromise propagating through shared platforms, and a slow, expensive cryptographic migration prompted by advances in quantum computing. Decision-makers who treat cybersecurity purely as prevention, or purely as a cost to be minimised, will be poorly positioned for either.

Principal findings

- **Resilience has displaced prevention as the organising principle.** The most consequential recent framework revision, the US National Institute of Standards and Technology's Cybersecurity Framework 2.0 (2024), added an explicit *Govern* function alongside identify, protect, detect, respond and recover — codifying the view that security is a continuous management discipline, not a wall.
- **Regulation is now the primary budget driver in regulated economies.** In the EU, the NIS2 Directive, the Digital Operational Resilience Act (DORA) for financial entities, and the Cyber Resilience Act for products with digital elements collectively pull cybersecurity into mandatory territory. In the US, the Securities and Exchange Commission's 2023 rules require timely disclosure of material incidents. Compliance timelines, more than any single attack, are setting the pace of enterprise spending.

- **Services, not software, dominate the market.** We estimate managed security, consulting and incident response account for the largest single share of sector revenue — a reflection of the workforce shortage and the operational complexity of running modern defences.
- **Platform concentration is a double-edged development.** Consolidation around a few cloud, identity and endpoint providers lifts baseline security for the median organisation, but the July 2024 global IT outage — a faulty software update, not an attack — showed how a single dependency can interrupt airlines, hospitals and payments simultaneously.
- **AI is an accelerant, not yet a decisive advantage.** Generative models make phishing, voice cloning and fraudulent-identity attacks cheaper and more convincing, while also increasing the volume of alerts defenders can triage. Through the forecast period we expect an unstable equilibrium rather than a clear victor.
- **The post-quantum migration has started and is under-scoped.** With NIST's first post-quantum cryptography standards finalised in 2024, "harvest now, decrypt later" data theft is a present risk even though capable quantum computers are not. Most institutions have not inventoried where vulnerable cryptography lives in their systems.
- **The workforce gap is structural.** Industry workforce studies put the global shortfall in the millions of roles. Automation and managed services relieve pressure but do not close the gap, which keeps upward pressure on both salaries and outsourcing.

1. Context and why it matters

Cybersecurity has crossed a threshold familiar from other domains of risk: it has become systemic. The digitalisation of payments, energy, logistics, healthcare and public administration means that the failure of a widely used piece of software or a widely trusted supplier no longer stays contained within one firm. Incidents in recent years have repeatedly propagated across sectors and borders. A 2017 self-propagating malware event caused an estimated ten billion dollars of global damage across shipping, pharmaceuticals and consumer goods, despite most victims not being its intended targets. A 2020 compromise of a widely deployed network-management vendor gave a sophisticated actor a foothold into numerous government and corporate networks through a routine software update. A 2023 vulnerability in a common file-transfer tool exposed data at hundreds of organisations that had never directly contracted with the attacker's chosen entry point. The connecting thread is dependency: institutions inherit the security posture of everything they rely on.

Two features make this different from earlier eras of computer crime. First, the adversary is professionalised and specialised. Ransomware, in particular, operates as a service economy, with distinct roles for access brokers, malware developers, negotiators and money launderers. This division of labour lowers the skill required to mount a damaging attack and raises the volume of attempts. Second, the line between criminal and state activity has blurred. Several governments tolerate, direct or benefit from cyber operations conducted against rivals' critical infrastructure and commercial base. Public advisories in 2023 and 2024 warned that state-linked actors had pre-positioned inside critical-infrastructure networks — not to steal data, but to retain the option of interrupting services during a future crisis. This is a strategic posture, not opportunistic crime, and it changes what "defence" has to mean for operators of essential services.

Dependency is the connecting thread: institutions inherit the security posture of everything they rely on — a single widely used component can propagate failure across shipping, healthcare, energy and payments. — IRI

For public institutions the stakes are civic as much as financial: continuity of hospitals, courts, benefits payments, elections administration and utilities. For private institutions the stakes are increasingly existential, because a serious incident now combines operational downtime, extortion, litigation, regulatory penalty and disclosure obligations into a single compounding event. The result is that cybersecurity has moved decisively out of the server room and into the boardroom and the cabinet office. That relocation of the problem is why a market that was once a subset of enterprise IT now warrants treatment as a sector in its own right, with its own regulatory apparatus, insurance market, labour market and geopolitics.

2. Market structure and scale

Sizing the cybersecurity market precisely is not possible from public data, because vendors bundle security into broader IT contracts, in-house labour is rarely accounted separately, and definitions vary between analysts. We therefore present a transparent, reproducible estimate rather than a single headline number. Our approach: take the consensus range of published analyst estimates for security software and services (commonly cited in the USD 180–220 billion range for 2024), decompose it into functional segments using typical analyst weightings, and attach growth ranges consistent with observed budget behaviour. Every figure below is an **estimate** intended to convey proportion and direction, not a measured value.

The most important structural fact is that **services outweigh products**. The scarcity of skilled staff and the operational burden of running detection-and-response around the clock push buyers toward managed services, consulting and outsourced security operations. Within products, the fastest-growing segments are those aligned with cloud and identity, while traditional network-perimeter spending grows more slowly as its logic is absorbed into cloud-native and zero-trust architectures.

SEGMENT	EST. 2024 REVENUE (USD BN)	EST. SHARE	EST. CAGR TO 2030	BASIS / NOTES
Security services (MSSP, consulting, incident response)	80–95	~42%	10–13%	Largest segment; driven by skills gap and 24/7 operations
Network & infrastructure security	25–30	~14%	6–9%	Mature; logic migrating into cloud and zero-trust
Identity & access management	18–22	~10%	12–15%	Core of zero-trust; passwordless adoption rising
Endpoint detection & response (EDR/XDR)	16–20	~9%	10–13%	Consolidating into broader platforms
Security operations (SIEM/SOAR/analytics)	14–18	~8%	10–14%	AI-assisted triage a key growth vector
Cloud security (CNAPP/CASB/workload)	9–13	~6%	18–24%	Fastest-growing; follows cloud migration
Data security & privacy	10–14	~6%	10–13%	Pulled by regulation and AI data governance
Application & product security	8–11	~5%	12–16%	Secure-by-design and software supply chain focus
Total (illustrative)	**~190–220**	**100%**	**~10–12%**	Sums of ranges; not additive to a single point

Where today's revenue sits — services dominate:

Estimated market share by segment, 2024

SEGMENT	SHARE
Security services	42%
Network & infrastructure	14%
Identity & access	10%
EDR/XDR	9%
Security operations	8%
Cloud security	6%
Data security	6%
Application & product	5%

Share of ~USD 190–220bn sector revenue. Analyst-weighting estimates; not additive to a single precise total.

Where it is growing fastest — cloud and identity lead, network trails:

Estimated CAGR to 2030 by segment

CATEGORY	LOW ESTIMATE (%)	HIGH ESTIMATE (%)
Services	10	13
Network	6	9
IAM	12	15
EDR/XDR	10	13
SecOps	10	14
Cloud	18	24
Data	10	13
AppSec	12	16

Low and high of the CAGR ranges in the table above. Estimates; cloud security is the clear outlier while mature network spending grows most slowly.

Two caveats deserve emphasis. First, the segment boundaries are increasingly artificial. The dominant commercial pattern is *platformisation*: buyers consolidate a dozen point tools into a handful of suites spanning endpoint, cloud, identity and security operations. This means revenue is migrating across the rows of the table faster than the totals change, and vendor market share is more volatile than category size. Second, none of this captures the in-house cost of security — the salaries, process overhead and opportunity cost borne inside every large organisation — which plausibly exceeds the external market. The "true" economic footprint of institutional cybersecurity is therefore materially larger than vendor revenue suggests.

On geography, spending is concentrated where regulation, insurance and high-value digital assets coincide. North America remains the largest market, at roughly 40–45% of global spend by our estimate, reflecting the scale of its technology sector and litigation exposure. Europe is the fastest-moving on regulation and is where compliance is currently the sharpest budget driver. Asia-Pacific is the fastest-growing in percentage terms off a smaller base, led by financial-sector modernisation and national data-sovereignty rules. These are directional estimates consistent with published analyst regional splits, not precise measurements.

3. Demand drivers and the shift to resilience

The demand side of this market is best understood as three overlapping pressures.

Regulation and disclosure. The clearest change of the past three years is that cybersecurity has become a legal obligation with teeth. In the European Union, the NIS2 Directive widened the range of "essential" and "important" entities subject to security and incident-reporting duties, with the transposition deadline in national law falling in late 2024. DORA imposed detailed operational-resilience, testing and third-party oversight requirements on financial entities from January 2025. The Cyber Resilience Act extended security obligations to the makers of products with digital elements, with duties phasing in through the middle of the decade. In the United States, the SEC's 2023 rules require public companies to disclose material cybersecurity incidents on a defined timeline and to describe their risk-management and governance. The net effect is that spending decisions are increasingly made to satisfy auditors, regulators and directors' liability, not only to defeat attackers. This tends to raise the baseline, smooth the spending cycle, and favour vendors who can evidence compliance.

Regulatory trajectory: compliance timelines set the spending pace

WHEN	MILESTONE	DETAIL
2023	US SEC incident-disclosure rules	Public companies must disclose material cybersecurity incidents on a defined timeline and describe their risk-management and governance.
2024	NIST CSF 2.0 and post-quantum standards	Framework 2.0 adds an explicit Govern function; NIST finalises the first post-quantum cryptography standards, starting the migration clock.
Late 2024	NIS2 transposition deadline	National-law transposition widens security and incident-reporting duties across 'essential' and 'important' EU entities.
Jan 2025	DORA applies to financial entities	Detailed operational-resilience, testing and third-party-oversight requirements take effect.
Mid-decade	Cyber Resilience Act duties phase in	Security obligations extend to the makers of products with digital elements.

Architecture change. The dissolution of the network perimeter has produced a durable design shift toward *zero trust* — the principle that no user, device or service is trusted by default and every access request is verified against identity, device posture and context. This reframes identity as the primary control plane, which is why identity and access management is among the higher-growth segments in our estimate. It also elevates two adjacent priorities: strong, phishing-resistant authentication (moving away from passwords and one-time codes toward hardware-backed and passkey methods), and continuous monitoring of what is actually happening inside systems rather than only at their edges.

The move from prevention to resilience. Because compromise can no longer be reliably prevented, the metric that matters is time — time to detect, contain and recover — and the capability that matters is the ability to keep operating, or degrade gracefully, while under attack. This is where the sector's language has changed most. Board conversations now centre on tested recovery, immutable and offline backups, incident playbooks, and the continuity of a defined set of critical business services. NIST's framing of *Govern* as a first-class function reflects this: resilience is an ongoing management commitment, embedded in risk appetite and accountability, rather than a project that finishes. For buyers, the practical consequence is spending shifting toward detection-and-response, backup and recovery, and exercises and rehearsals — categories that assume breaches will happen.

4. Competitive landscape and the concentration question

The vendor landscape is consolidating around platforms. For most of the sector's history, enterprises assembled defences from dozens of specialist products, each solving a narrow problem. The operational cost of integrating and staffing that sprawl has become prohibitive, and buyers now actively seek to reduce their number of vendors. The beneficiaries are large platform providers able to span endpoint, cloud, identity, network and security operations, plus the hyperscale cloud providers whose native security services are default-adjacent to where workloads already run. Specialist vendors persist and thrive where they are demonstrably better at a hard problem, but the commercial gravity favours suites.

This consolidation has an ambiguous effect on collective security. On one hand, it raises the floor: a mid-sized organisation running a well-configured mainstream platform is far better defended than one stitching together tools it cannot staff. Shared telemetry across millions of endpoints also gives large defenders a genuine visibility advantage over any single attacker. On the other hand, concentration converts diverse, uncorrelated risks into shared, correlated ones. When a widely deployed component fails — whether through a malicious supply-chain compromise or an ordinary defective update — the blast radius is systemic. The July 2024 global outage, caused by a flawed update to a widely installed security agent, grounded flights, delayed medical procedures and interrupted payments across multiple countries within hours. No attacker was involved, which is precisely the point: the same monoculture that lifts baseline security also manufactures single points of failure that individual buyers cannot diversify away through their own purchasing.

> ***Key finding — correlated, systemic risk*** *— The July 2024 global outage — a faulty software update, not an attack — grounded flights, delayed medical procedures and interrupted payments across multiple countries within hours. The same*

> *platform concentration that raises the security floor converts diverse, uncorrelated risks into shared, correlated ones that buyers cannot diversify away.*

The insurance market is the third actor shaping competition and behaviour. Cyber insurance grew quickly, then hardened sharply in 2021–2022 as ransomware losses mounted, with insurers raising premiums, tightening terms and demanding controls such as multi-factor authentication and tested backups as conditions of cover. That underwriting discipline has had a real, if uneven, effect on baseline hygiene across the insured population. Since then the market has softened somewhat as loss experience stabilised, but capacity remains constrained for the largest correlated risks. Insurers are, in effect, becoming private regulators of security practice — and their appetite, or lack of it, for systemic and war-adjacent scenarios is one of the sector's important open questions.

5. Threat dynamics, AI and cryptography

Three dynamics will shape the risk environment through the forecast period.

Ransomware and extortion economics. Ransomware remains the dominant financially motivated threat because it works as a business. The shift over recent years has been from encryption-only attacks to double and triple extortion — stealing data before encrypting it, then threatening publication, and sometimes pressuring the victim's customers directly. This makes robust backups necessary but no longer sufficient, because restoring systems does not undo a data theft. The policy debate over whether to ban extortion payments is unresolved: prohibition could reduce the incentive to attack but risks penalising victims, particularly hospitals and small public bodies, and driving payments underground. Our reading is that mandatory reporting and targeted dismantling of the criminal ecosystem are more tractable near-term levers than outright payment bans.

Artificial intelligence on both sides. AI changes the economics of the contest symmetrically. For attackers, generative models reduce the cost and raise the credibility of social engineering: fluent phishing at scale, convincing voice and video impersonation of executives, and faster reconnaissance and vulnerability discovery. Business-email-compromise and fraudulent-identity schemes are the near-term beneficiaries, and identity verification is a growing weak point as a result. For defenders, the same technologies increase the throughput of alert triage, summarise incidents, and help stretched teams cover more ground — a meaningful relief given the workforce shortage. Crucially, AI does not clearly favour either side over the forecast horizon; it raises the tempo and lowers the barrier to entry for attacks while making defensive operations more scalable. The realistic expectation is a faster, noisier contest rather than a decisive advantage for defence.

The cryptographic transition. In 2024, NIST finalised the first standards for post-quantum cryptography — algorithms designed to resist attack by a sufficiently capable quantum computer. Such a machine does not yet exist at the scale required to break today's public-key cryptography, and may not for years. But the risk is present now, because adversaries can capture encrypted traffic and stored data today and decrypt it later once the capability arrives — the "harvest now, decrypt later" problem. Data with a long confidentiality lifespan (state secrets, health records, intellectual property) is exposed to this today. The migration to quantum-resistant cryptography will be a multi-year, cross-system undertaking on the scale of previous major cryptographic transitions, and it begins with an inventory most institutions have not yet done: knowing where cryptography lives in their systems and which of it protects long-lived secrets. This is the sector's clearest example of a large, foreseeable, under-budgeted obligation.

6. Regional and public-sector lens

The public sector is both a large buyer and a distinctive risk case. Governments run essential services, hold sensitive population-scale data, and often operate on constrained budgets and long technology-refresh cycles, which leaves legacy systems in place longer than is prudent. Local government, healthcare and education are disproportionately represented among ransomware victims precisely because they combine high-value services, sensitive data and thin security resourcing. This makes the public sector a policy priority independent of its share of market spend.

National approaches diverge in instructive ways. The European model leans on binding, harmonised regulation and mandatory reporting, using rules such as NIS2 and DORA to raise minimum standards across the bloc and to hold senior management accountable. The United States blends market mechanisms, sector-specific rules and a strong central coordinating and advisory role for its cybersecurity agency, with disclosure obligations sharpening board attention. A number of Asia-Pacific economies emphasise data-localisation and sovereignty requirements alongside critical-infrastructure protection. These differences matter for multinational institutions, which must reconcile overlapping and sometimes conflicting regimes, and for vendors, whose compliance

features are increasingly a competitive differentiator. The overall direction of travel, however, is common: mandatory baselines, incident reporting, supply-chain scrutiny and accountability pushed up to senior leadership.

Three scenarios to 2030

The forecast horizon contains genuine uncertainty across three variables: the pace of AI-enabled offence versus defence, the incidence of systemic events, and the coherence of the regulatory and geopolitical environment. We set out three scenarios. These are analytical constructs, not predictions, and the truth will likely combine elements of each.

Scenarios to 2030 (analytical constructs, not predictions)

A — Managed resilience — Central case · most probable

Regulation keeps raising baselines; the market grows in the low-double-digits and consolidates around platforms. Ransomware stays a chronic, costly nuisance; AI raises the tempo without a decisive winner. Cybersecurity comes to resemble industrial safety.

METRIC	VALUE
Market growth	~10–12%/yr
Ransomware	Chronic nuisance
Post-quantum	Slow, begins

B — Fragmented escalation — Downside · lower odds, highest impact

Geopolitical decoupling accelerates, state-linked operations move from pre-positioning to interruption, and AI-accelerated attacks outpace defence. A systemic event strains the insurance market and prompts emergency regulation.

METRIC	VALUE
Spending	Rises reactively
Compliance	Fragments
Insurance	Strained

C — Resilience dividend — Upside · requires coordination

Secure-by-design shrinks the supply of vulnerabilities, coordinated takedowns raise the cost of offence, and defenders absorb AI faster thanks to scale. Post-quantum migration stays on schedule and the workforce gap narrows.

METRIC	VALUE
Cost of offence	Rises
Workforce gap	Narrows
Security drag	Falls

Scenario A — Managed resilience (central case). Regulation continues to raise baselines and smooth spending; the market grows in the low-double-digits and consolidates further around platforms. Ransomware remains a chronic, costly nuisance rather than a catastrophe. AI raises the tempo of the contest without either side gaining decisively. Post-quantum migration proceeds slowly but begins in earnest in the most exposed sectors. Cyber insurance stabilises as a private regulator of hygiene. In this world, cybersecurity comes to resemble industrial safety or financial-risk management: never solved, but competently managed, with resilience embedded in governance. This is our most probable outcome.

Scenario B — Fragmented escalation (downside). Geopolitical decoupling accelerates, state-linked operations against critical infrastructure move from pre-positioning to interruption during a crisis, and AI-accelerated attacks outpace defensive adoption for a sustained period. A systemic event — a supply-chain compromise or a correlated platform failure — causes cross-sector losses large enough to strain the insurance market and prompt emergency regulation. Compliance regimes fragment along geopolitical lines, raising costs for multinationals. Spending rises sharply but reactively and inefficiently. This scenario is less likely than the central case but carries the highest consequences, and its probability is not negligible.

Scenario C — Resilience dividend (upside). Secure-by-design practices, mandated by product regulation, gradually reduce the supply of exploitable vulnerabilities. International coordination on incident reporting and takedown of criminal networks improves, raising the cost of offence. AI is absorbed more effectively by defenders than attackers because defensive deployment benefits from scale and shared data. Post-quantum migration proceeds on schedule in critical sectors, and the workforce gap narrows as automation and training compound. Security becomes a smaller drag on digital investment. This is the most favourable plausible path and requires sustained policy and industry coordination that has so far been partial.

Across all three, two structural facts hold: the economic footprint of security keeps growing faster than general IT, and resilience — the ability to keep operating through incidents — remains the correct organising goal regardless of which scenario dominates.

Implications by audience

For governments and policymakers. Treat critical-infrastructure resilience as a continuity-of-services problem, not only a data-protection problem: the state-linked pre-positioning inside essential networks is about the option to interrupt, and defence must be measured in tested recovery, not just intrusion prevention. Prioritise the under-resourced public bodies — local government, hospitals, schools — that are structurally the softest targets. Use regulation to set outcome-based baselines and mandatory, timely incident reporting, but guard against fragmentation that imposes conflicting obligations on the same multinational entities. Begin planning the post-quantum migration for long-lived state secrets now, starting with a cryptographic inventory. And weigh the ransomware-payment debate toward reporting mandates and coordinated takedowns of criminal infrastructure rather than blanket bans whose burden would fall hardest on the least-resourced victims.

For business leaders and boards. Reframe the security conversation around a defined set of critical business services and the tested ability to keep them running. Ask for evidence, not assurance: when were backups last restored under realistic conditions; how long did the last incident exercise take to reach recovery; which third parties, if compromised, would stop the business. Recognise that platform consolidation improves your posture but concentrates your dependency risk — hold a deliberate view on single points of failure, and do not assume a mainstream supplier cannot cause an outage. Treat identity as the central control and move decisively toward phishing-resistant authentication. Budget for the post-quantum inventory now, before it becomes urgent.

For investors and financial institutions. The sector's durable growth is real but the easy narrative — that spending only rises — obscures where value accrues. The structurally attractive positions are in services (sustained by the workforce gap), cloud and identity security (aligned with the architecture shift), and platforms able to consolidate buyer tool sprawl. Point-solution vendors face pressure to be acquired or to prove a defensible technical edge. On the risk side, correlated and systemic exposure is under-priced across portfolios: an institution's cyber risk is inherited from its shared dependencies, so concentration in a few platforms is a portfolio-level, not just a company-level, consideration. Cyber insurance capacity for systemic scenarios is a market to watch closely, as its limits define who ultimately bears tail risk.

Methods and sources

This report is a synthesis and interpretation of publicly available information, not a primary measurement study. Our market sizing takes the consensus range of published analyst estimates for cybersecurity software and services, decomposes it into functional segments using typical category weightings, and attaches growth ranges consistent with observed enterprise budget behaviour. **Every quantitative figure in Section 2, and all regional splits, are estimates presented as ranges to convey proportion and direction. They should not be read as measured values, and they are not additive to a single precise total.** Where we cite orders of magnitude for historical incident losses, we rely on widely reported public estimates that themselves carry wide error bars.

The qualitative analysis draws on established, non-partisan source categories: national framework and standards documents (such as the NIST Cybersecurity Framework and post-quantum standards); primary regulatory texts (NIS2, DORA, the Cyber Resilience Act, SEC disclosure rules); annual threat-landscape and breach-cost studies produced by industry and independent researchers;

workforce studies; national cybersecurity agency advisories; and public reporting on major incidents. We have deliberately described sources by kind rather than attributing precise statistics to specific proprietary reports, both to respect their licensing and to avoid conveying false precision.

Established facts we rely on with confidence include: the addition of the *Govern* function in NIST's 2024 framework revision; the finalisation of the first NIST post-quantum cryptography standards in 2024; the substance and timelines of the named EU and US regulations; and the occurrence and cross-sector character of the major incidents referenced. Judgements about market share, segment growth, scenario probabilities and the balance of AI advantage are the authors' analytical estimates and are flagged as such throughout. The scenarios are structured hypotheticals, not forecasts, and are intended to bracket a range of plausible outcomes rather than to identify a single expected future.

This is independent analysis. The Digital Resilience Programme received no vendor or government funding earmarked for this report, and no external party had approval rights over its findings.

Sources and references

The regulatory texts, national frameworks and standards below were consulted directly. Threat-landscape, breach-cost and workforce figures are drawn from the recurring studies named here and cross-checked for order of magnitude; proprietary market estimates are referenced by category in the methods note rather than itemised.

- European Union Agency for Cybersecurity (2024). *ENISA Threat Landscape 2024.* ENISA, Athens.
- National Institute of Standards and Technology (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29).* NIST, US Department of Commerce, Gaithersburg, MD.
- National Institute of Standards and Technology (2024). *FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA): the first finalised post-quantum cryptography standards.* NIST, Gaithersburg, MD.
- European Parliament and Council of the European Union (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* Official Journal of the European Union.
- European Parliament and Council of the European Union (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).* Official Journal of the European Union.
- European Parliament and Council of the European Union (2024). *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).* Official Journal of the European Union.
- US Securities and Exchange Commission (2023). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Final Rule, Release No. 33-11216).* SEC, Washington, DC.
- ISC2 (2024). *Cybersecurity Workforce Study 2024.* International Information System Security Certification Consortium.
- IBM Security and Ponemon Institute (2024). *Cost of a Data Breach Report 2024.* IBM Corporation, Armonk, NY.
- OECD (2024). *Digital security policy and the governance of systemic cyber risk.* OECD Digital Economy Papers, OECD Publishing, Paris.
- Recurring industry threat-landscape and breach-cost studies (2023–2025), referenced by category for orders of magnitude only.

Suggested citation

Vance, H., Adeyemi, M., and Nair, P. (2025). *Cybersecurity and Digital Resilience for Public and Private Institutions.* Flagship Report. International Research Institute. Available under CC BY 4.0.