WHY CYBERSECURITY FAILS:

THE CULTURAL AND STRATEGIC IMPERATIVE

CACI

Cybersecurity breaches continue to plague organizations worldwide despite decades of advancements in security technologies and increasing investments. In 2023 alone, there were over 3,200 publicly reported data compromises impacting more than 353 million individuals – a staggering 78% increase from the prior year. The global cost of cybercrime is projected to reach an astonishing $10.5 trillion by 2025, with the average cost per data breach hitting a record $4.88 million in 2024. These figures span all sectors – from financial services and healthcare to manufacturing and government – underscoring that no industry or region is immune. Paradoxically, many victim organizations *were* formally compliant with security regulations or certified against industry standards at the time of their breaches.

This raises a critical question: Why are cybersecurity efforts so often failing, even in organizations that tick all the right compliance boxes?

This paper argues that the root cause lies in a systemic, historical flaw: businesses have treated cybersecurity primarily as a compliance checklist exercise rather than cultivating it as an integral part of organizational culture and risk management. Too many firms equate passing audits or obtaining certificates with being secure, when in reality compliance does not equate to actual security. As one cybersecurity expert bluntly put it, “Compliance becomes a milestone – not a mindset” in such organizations. The result is *cybersecurity theatre* – an illusion of safety on paper that masks serious vulnerabilities in practice.

In the sections that follow, we explore the historical and systemic reasons behind these failures. We examine prominent case studies across industries – including healthcare, finance, and manufacturing – that illustrate how superficial, checkbox approaches lead to repeated incidents. We then analyse emerging trends and data that highlight the consequences of this mindset. Finally, we present strategies and frameworks for fundamentally changing course: embedding cybersecurity into corporate culture and governance, elevating it to a board-level strategic priority, and integrating it across business units for long-term resilience.

The discussion draws on recent research findings, government policy developments, and expert commentary to offer actionable insights for business and technical leaders alike.

From the early days of information security regulations, organizations frequently adopted a minimalist, compliance-driven stance toward cybersecurity. Industry and government frameworks such as the Payment Card Industry Data Security Standard (PCI DSS), HIPAA, and ISO/IEC 27001 were designed to establish foundational controls. These standards were never intended to represent the full extent of a security program, but rather to provide a baseline upon which more mature and adaptive strategies could be built. However, many firms misinterpreted them as the final destination rather than the starting line. The prevailing mentality became "get the cert, full stop" instead of embracing continuous, risk-informed improvement.

Internal security programs consequently became preoccupied with passing audits and accumulating compliance credentials, sometimes treating preparation as a kind of "theatre production" aimed more at appeasing auditors than reducing actual threat exposure. In some cases, documentation was polished to perfection while controls were inconsistently implemented or poorly enforced. Security thus devolved into a one-time or annual project instead of a lived, daily discipline woven into decision-making and behaviour across the organization. This compliance-centric mentality created a dangerously false sense of security. Passing an audit or receiving a compliance certificate was equated with being safe from threats, when in reality, these indicators merely reflected the ability to demonstrate conformity at a single point in time. As one widely cited analysis observed, "Passing an audit doesn't mean you're secure. It means you're auditable." This subtle but critical distinction continues to be lost on many leadership teams.

Organizations ticked the boxes by deploying basic technologies – firewalls, antivirus, access policies – but often neglected to examine or mitigate risks that fell outside the narrow lens of compliance assessments. They met the literal requirements of regulatory frameworks but failed to internalize their underlying intent: dynamic, risk-based protection. In some cases, adherence to standards even backfired by broadcasting to attackers what security controls were most likely in place, enabling adversaries to bypass them by targeting the unregulated periphery. These oversights became tragically evident in breaches like the one that hit Target in 2013. Despite passing PCI audits and maintaining the necessary controls, attackers were able to exploit weak points outside the standard's scope. As noted in a SANS Institute case study, truly comprehensive security "will consider all assets, not just those that fall under compliance regulations." Limiting protections only to those systems under audit leaves vast segments of the digital estate vulnerable – a lesson Target and many others have learned the hard way.

Historically, senior leadership compounded these vulnerabilities by viewing cybersecurity primarily as a technical burden or compliance obligation that could be delegated. Boards and C-suite executives were often satisfied once the requisite paperwork was filed or the certifications secured, rarely questioning the substance of what those controls truly achieved. A recurring pattern emerged: "leadership teams don't understand cybersecurity, so instead of technical leadership, they appoint someone who can 'own the compliance project.'" Instead of hiring experienced cybersecurity professionals to lead, organizations sometimes assigned program managers – even those from unrelated fields like marketing or operations – to manage security, prioritizing interpersonal polish and report-readiness over depth of expertise.

The result was often what one observer memorably described as "a Frankenstein program stitched together with template policies, copy-pasted risk registers, and vendor promises." On paper, the security program appeared cohesive and well-structured. In practice, it lacked coordination, lacked vision, and lacked effectiveness. Superficially reassuring dashboards hid the fact that essential gaps in monitoring, incident response, or vulnerability management were going unaddressed.

This wilful ignorance – wrapped in a slick veneer of compliance – is no longer sustainable. As adversaries grow more sophisticated and attack surfaces expand, these shallow approaches are driving companies toward what experts now warn may become "a multi-billion-dollar disaster" marked by large-scale breaches, irreversible trust erosion, and profound operational disruption. Without meaningful cultural and strategic change, organizations risk remaining locked in a dangerous cycle of performative security, perpetually vulnerable beneath a polished but hollow shell.

The compliance-first approach flourished in part because organizational culture around cybersecurity was weak or toxic. In many companies, security was siloed within IT departments, far removed from core business strategy. Employees and even mid-level managers came to regard security measures as obstacles to "get around" or as merely an annual training annoyance, rather than an essential shared responsibility. Leadership failed to set the tone from the top. In cases like the UK's National Health Service (NHS) before the 2017 WannaCry attack, most hospital and trust boards "took little ownership of cybersecurity matters". Cyber risk was not seen as a boardroom issue or a patient safety issue. Indeed, a post-mortem on WannaCry found that *"most [NHS] trusts did not even think that cybersecurity was a risk to patient outcomes"* – a "naive and dangerous view" in today's digital healthcare environment.

Such a cultural blind spot at the leadership level meant vital security warnings went unheeded. NHS Digital had issued urgent alerts and patches prior to WannaCry, yet management failed to act, leaving many systems unpatched and vulnerable. The result was a massive ransomware outbreak that disrupted services across dozens of hospitals – a crisis not of technology per se, but of management and culture.

Lack of clear accountability compounded these issues. When everyone assumes someone else is handling cybersecurity, critical tasks fall through the cracks. In the Equifax 2017 breach – one of history's largest – a congressional investigation blamed a "*culture of cybersecurity complacency*" at the company. Equifax had ample warning of a critical Apache Struts software vulnerability months before hackers exploited it, yet failed to ensure the patch was applied across all systems. No single executive took charge of verifying remediation. Furthermore, hundreds of security certificates had lapsed at Equifax, including one that would have detected the data exfiltration – but it had been expired for 19 months with no one accountable for renewal.

The House Oversight Committee report concluded that Equifax *"failed to fully appreciate and mitigate its cybersecurity risks"* and did not follow an adequate security program, directly contributing to the breach. In effect, security was nobody's job at the senior level – or at best, it was a secondary responsibility easily overlooked. Such governance failures stem from a cultural disconnect where cybersecurity isn't truly valued or understood by top leadership.
Another systemic factor is the "tick-the-box" performance measurement of security teams, which often incentivizes the wrong outcomes.

If security personnel are rewarded primarily for passing audits or meeting compliance metrics, they may focus on those narrow goals rather than broader risk reduction. Organizations have historically measured security success by absence of compliance findings or by how many policies are in place, rather than by more meaningful indicators (e.g. time to detect incidents, percentage of assets properly secured, employee phishing resilience scores, etc.). This creates a complacent environment where, as critics note, "movement is mistaken for progress" – lots of security paperwork and meetings occur, but the company isn't actually safer.

Over time, talented cybersecurity professionals grow frustrated in such environments ("*checklist administrators rather than mission-critical leaders*") and may leave, further weakening organizational capability. Indeed, industry observers have warned of a *"talent exodus"* from companies with poor security culture. All of these issues feed a vicious cycle: superficial compliance efforts lead to breaches, which lead to leadership crises and fire drills, but once the dust settles the organization often goes back to the same compliance-driven approach without addressing root cultural issues.

The historical bias toward compliance has left organizations increasingly flat-footed in the face of rapidly evolving cyber threats. Attackers today are not only more aggressive, but also better resourced, highly organized, and adept at exploiting precisely the types of gaps that a checkbox approach tends to overlook. Instead of confronting only systems within a defined compliance scope, they target human vulnerabilities, third-party supply chain partners, and sprawling "shadow IT" systems that exist outside the purview of formal audits or oversight. For example, ransomware operators and nation-state adversaries care little whether an organization passed last year's compliance audit – they look for any exploitable opening, whether it's an unmonitored device, a forgotten application instance, or an unsuspecting employee who clicks a phishing link. A reactive stance, focused on legacy compliance checklists and outdated risk models, is ill-suited to counter such adaptive, persistent adversaries.

This misalignment is visible in the rising frequency and severity of "mega-breaches" and destructive attacks that have unfolded over the past decade. Many organizations remain locked in a reactive cycle – scrambling after each incident to patch vulnerabilities and restore systems, rather than proactively hardening environments and building systemic resilience. This operational posture reflects a broader failure to evolve security practices beyond compliance minimums. A 2025 industry benchmarking study revealed that even in some of the most tightly regulated sectors, such as healthcare, most organizations remain stuck in this reactive mode. For instance, the NIST Cybersecurity Framework's Respond and Recover functions were relatively well implemented, indicating an ability to manage and mitigate breaches once they occurred. However, foundational capabilities – such as risk governance, asset identification, and proactive threat modelling – were far less mature. In healthcare specifically, coverage for third-party risk management and asset management hovered around just 52 to 53% among surveyed providers. This means nearly half of organizations lacked even a basic, complete inventory of their own systems or a clear understanding of the risks posed by external vendors. Such gaps are symptomatic of a broader trend that spans industries: compliance routines (e.g. HIPAA or PCI checklists) have failed to drive truly robust, end-to-end security practices where they matter most.

As cyber threats grow more sophisticated – incorporating tactics like AI-powered malware, advanced persistent threats, and software supply chain compromises – the gap between "secure enough to pass an audit" and "genuinely secure against real-world attackers" is widening into a dangerous chasm. Threat actors increasingly seek out companies that have just barely cleared the compliance bar, rightly assuming that these organizations have implemented surface-level controls but lack true depth in detection, response, and resilience. In other words, doing the bare minimum is no longer neutral – it actively increases an organization's risk exposure.

This trend is further exacerbated by the rise of new attack vectors that fall outside traditional compliance boundaries. Cloud misconfigurations, vulnerabilities in IoT devices, and sophisticated social engineering campaigns rarely feature in conventional audit frameworks. As a result, organizations that focus too narrowly on ticking regulatory boxes often develop an inflated sense of readiness. They believe their risk posture is sufficient when, in reality, they may be ill-prepared for the actual threat landscape.

One survey of 151 senior corporate executives underscored this disconnect. While 71% of respondents believed their cybersecurity funding was "adequate or high," only 39% felt their board had a proactive or informed understanding of cybersecurity risks. Even more concerning, just 31% considered their organizations to be early adopters of cybersecurity innovations or adaptive strategies. In essence, leadership teams believed they were doing enough – investing in tools and passing audits – yet the underlying security maturity of their organizations remained underdeveloped. This widespread overconfidence, nurtured over years of conflating regulatory compliance with genuine security, can prove fatal when tested by the scale, speed, and sophistication of modern threats.

.

Cybersecurity failures induced by the compliance-focused mindset have played out in virtually every industry. Below we examine several notable cases – in finance, healthcare, and manufacturing/critical infrastructure – to illustrate common patterns and lessons.

Financial Services: Equifax and the "Complacency" Breach

The Equifax breach of 2017 stands as a stark example of how a lax security culture can neutralize the effects of formal compliance. Equifax, one of the largest credit reporting agencies, lost personal data on 148 million Americans (and many more globally) in a single incident. Equifax was subject to myriad regulations (GLBA, FTC safeguards, etc.) and had passed audits; on paper, it had a security program. In practice, however, investigators found a shocking level of negligence. A House Oversight Committee report described a *"culture of cybersecurity complacency"* at Equifax.

Management had received an urgent Department of Homeland Security alert about a critical Apache Struts web server vulnerability in March 2017, yet failed to ensure all systems were patched. One business unit simply did not do its updates, and no effective mechanism existed to track or enforce the patching compliance. Equifax also allowed over 300 security certificates to expire, including the one monitoring outbound network traffic. Because an intrusion detection device's certificate had been invalid for 19 months, the attackers' data exfiltration went unnoticed for 76 days. These basic lapses indicate a lack of accountability and oversight, not a lack of written policies. In fact, Equifax had policies – but no one followed through to implement or audit them in practice. The congressional report concluded that Equifax's failure to **"**follow an adequate security program" and address known issues directly enabled the breach. Put simply, Equifax leaders knew of critical risks and did little – a fatal cultural failing.

Financial institutions are generally steeped in compliance regimes, yet Equifax shows that even in such environments, security can fail if treated as a checkbox. A post-breach statement from Equifax attempted to dispute some investigative findings, but notably the company agreed with many recommendations around governance and oversight. Since the breach, Equifax claimed to have made security a top enterprise priority, including board-level engagement. It had little choice – the reputational damage and regulatory fallout (fines, lawsuits) were immense. Equifax became a "poster child" for stronger data protection laws and even discussions of jailing executives for egregious security failures.

The financial impact was also severe: immediate cleanup and legal costs exceeded $1.4 billion, not to mention the hard-to-quantify loss of customer trust. The key lesson from Equifax is that paper compliance cannot compensate for a poor security culture. A company dealing in highly sensitive data must go beyond ticking boxes to ensure genuine accountability, continuous risk monitoring, and empowerment of security teams – from the CISO down to IT admins. Equifax had the resources to do this, but not the mindset; as the report said, it *"failed to appreciate"* its cyber risks, illustrating a classic complacency born of superficial governance.

Retail: Target's PCI Compliance vs. Actual Security

The retail sector offers another instructive case. Target Corp.'s 2013 breach, in which some 40 million payment card numbers were stolen, showed how meeting industry standards is not enough if those standards are treated as a ceiling. Target was required to comply with the PCI DSS, and in fact Target had passed its PCI audits prior to the breach. The company had invested in security tools and was ostensibly following the rules. Yet attackers still managed to infiltrate Target's network (via a third-party HVAC contractor's credentials) and install malware on point-of-sale terminals, siphoning off millions of customers' card data. How? Subsequent analysis revealed multiple failures beyond PCI's narrow focus.

Target's network segmentation was inadequate, allowing attackers who breached a vendor access to pivot into the payment system. Several *internal alerts were overlooked or ignored* by Target's security staff during the attack's early stages, suggesting an incident response process that was more checkbox than reflex. Notably, Target's expensive threat detection system (FireEye) did trigger alarms, but the alerts were not acted upon. This indicates a lack of proper training, staffing, or empowerment of the security operations team – again a cultural issue, not a compliance one.

Crucially, Target's security strategy was heavily oriented around PCI requirements, to the detriment of broader risk management. The company focused on protecting cardholder data per PCI rules, yet the attackers found entry through systems and vendors outside PCI scope. One post-breach report observed: *"Target's strategy focused mainly on PCI compliance, while there are sometimes risks that fall outside of the scope of PCI requirements."* In other words, Target did "what was mandated for a subset of assets" (the cardholder environment) but failed to consider threats to other assets and pathways. The lesson – echoed by experts – is that compliance must be the floor, not the ceiling of security effort. Had Target embraced a culture of continual risk assessment, it might have extended multifactor authentication and network segregation to vendor connections, or heeded internal red flags of suspicious activity. Instead, the narrow compliance mindset left it blind to obvious weaknesses. The fallout included an $18.5 million settlement with dozens of state attorneys-general, the CEO's resignation, and $252 million in total costs in the first year. Target did eventually overhaul its security program, including appointing a new executive for cyber risk, but the breach had already done lasting damage. This case underscores that "being compliant" is not the same as being secure, and treating it as such invites failure.

Healthcare: The NHS and Reactive Posture

Healthcare organizations, holding life-critical systems and sensitive patient data, face unique challenges – but their security failures often trace back to the same root problem. The WannaCry ransomware outbreak of May 2017 crippled large parts of Britain's National Health Service, disrupting dozens of hospitals and causing an estimated 19,000 appointment cancellations. WannaCry was a relatively unsophisticated attack (it exploited a known Windows vulnerability for which a patch existed). The real failure was one of governance and preparedness: many NHS sites had not applied the available patches, and the health system lacked an effective incident response plan for a cyber emergency. A parliamentary inquiry concluded that NHS leadership had been warned repeatedly about cyber risks but did not act. In fact,

NHS Digital (the central IT authority) had offered on-site cybersecurity assessments to 88 regional NHS trusts in the year before WannaCry – and every single one failed those assessments. However, because NHS Digital had *no enforcement power*, and cybersecurity wasn't part of the Care Quality Commission's hospital inspection regime, local managers simply did not prioritize fixing the issues. This exemplifies a classic compliance gap: if something isn't formally required or audited, it falls by the wayside. NHS boards were focused on clinical targets and budgets, while cyber defence was "out of sight, out of mind." The NAO (National Audit Office) report diplomatically labelled this a top-level management failure, not just an IT failure. In short, leadership's failure to embed cybersecurity into the organizational culture and governance left the door wide open.

Once WannaCry hit, the cultural unpreparedness manifested in chaos: some hospitals literally shut down their networks as a precaution (even those not infected) because they had no confidence in containment measures. Communication broke down – with email offline, staff resorted to WhatsApp and phone calls. It became evident that decentralization without oversight had left NHS cybersecurity "very exposed". No mechanism existed to ensure that critical alerts and patches from NHS Digital were acted upon; many warnings were likely lost amid other administrative noise. Perhaps most tellingly, NHS Digital's own post-incident review found that *most NHS entities did not perceive cyber threats as risks to patient safety*.

This highlights a dangerous cultural disconnect – one that is thankfully beginning to change in healthcare, as regulators tighten requirements and as high-profile hospital ransomware attacks endanger patient care. For example, the United States has ramped up enforcement of the HIPAA Security Rule and pushed hospitals to adopt frameworks like NIST's guidelines. Yet even with regulations, healthcare breaches have surged. In 2023, there were 725 reported healthcare breaches in the U.S., exposing over 133 million medical records – the most ever. By 2024, that number of records more than doubled again (due to a few mega-breaches), showing the stakes are climbing. It's clear that check-the-box compliance with HIPAA alone has not prevented breaches.

Only by changing the culture – treating cyber risk as intrinsic to patient care quality and institutional governance – can healthcare turn the tide. Encouraging signs include more healthcare boards recruiting cybersecurity expertise and government initiatives like the HHS 405(d) Health Industry Cybersecurity Practices, which emphasize enterprise-wide risk management over mere compliance. The NHS, for its part, did treat WannaCry as a wake-up call; funding for NHS

cybersecurity was boosted and structural changes were recommended. But as the NAO warned, *"there will definitely be a next time"* if broad lessons aren't learned.

Manufacturing & Critical Infrastructure: Lessons from NotPetya

Perhaps the most dramatic illustration of cybersecurity failure across sectors was the NotPetya malware attack of 2017. NotPetya was a destructive worm initially aimed at Ukrainian infrastructure, but it cascaded globally, hitting companies in manufacturing, shipping, pharma, energy, and more. Within hours, the malware brought multinational giants to their knees: shipping conglomerate Maersk, pharmaceutical maker Merck, logistics provider FedEx/TNT, food producer Mondelēz, and others suffered massive outages and losses. The White House estimated NotPetya caused over $10 billion in total damages worldwide.

While NotPetya was a state-sponsored cyberweapon with extraordinary impact, its success was abetted by the poor cybersecurity practices prevalent in many large firms – especially those outside the tech/finance realm. For example, Maersk, the world's largest container shipping company, was among the hardest hit. Maersk prides itself on operational excellence in shipping, but its digital security posture in 2017 was relatively immature. Reports revealed that numerous Maersk servers had not been updated or patched for four years or more prior to NotPetya. The company's network was flat and interconnected enough that once the worm got in (via a compromised Ukrainian tax software update), it spread enterprise-wide in minutes. One executive noted that 55,000 PCs and 7,000 servers were essentially destroyed in roughly 7 minutes after NotPetya obtained domain administrator credentials and propagated itself. No amount of last-minute scrambling could have stopped this kind of lateral movement given the lack of internal segmentation and privileged access controls.

Importantly, Maersk was *not oblivious* to cybersecurity – in fact, by some accounts it had patched the specific Windows vulnerability (EternalBlue) that WannaCry had used. But patching alone was insufficient. NotPetya cleverly used multiple propagation methods (including stealing admin passwords, as happened with the MeDoc server at Maersk). This revealed that Maersk's defences were one-dimensional; they hadn't anticipated or mitigated scenarios beyond the known vulnerability du jour. In hindsight, Maersk's tech leaders cited several missing pieces: better network isolation, real-time anomaly detection, and (especially) rigorous management of privileged accounts. At the time of NotPetya, Maersk's board likely saw cybersecurity as an IT issue, not something requiring enterprise-wide drills or investment akin to safety protocols. That culture changed abruptly after the disaster – Maersk's recovery, which impressively restored operations in about 10 days, was followed by a comprehensive security transformation and a much larger security team. Andy Powell, Maersk's CISO hired post-NotPetya, expanded the security headcount from 28 to 150 and implemented modern controls.

The company also became unusually candid about sharing lessons learned: their CTO urged that "Company boards and audit committees need to understand this stuff is real" – cyber attacks can devastate core business operations, not just steal data. This is a cultural awakening many industrial and manufacturing firms have since experienced, as ransomworms and nation-state threats target them. Nevertheless, across critical infrastructure sectors, many organizations remain far behind on cybersecurity hygiene and culture. Industrial control systems often run on legacy technology, and until recently there was scant regulatory push for cyber resilience in these areas. Initiatives like the U.S. NIST Cybersecurity Framework and various sector-specific guidelines (e.g. for utilities, transportation) are gradually encouraging better practice. But the NotPetya episode proves that complacency and delayed action can exact catastrophic costs. Firms that rely on outdated, unpatched systems and assume "it won't happen to us" are simply ticking time bombs. In manufacturing and beyond, the mantra must shift from *"it's an IT problem"* to *"it's a fundamental business risk we must manage continuously."*

The Cost of Superficial Security and Emerging Trends

The case studies above highlight how a superficial approach to cybersecurity – doing the minimum and treating it as a low priority – leads to repeated failures. Across sectors, certain common patterns emerge from these failures: unpatched systems, unheeded warnings, weak oversight, slow response, and ultimately severe business harm. The *direct* costs of breaches are soaring (legal fees, penalties, technical recovery, customer notification, etc.), but the *indirect* costs like reputational damage and operational downtime can be even more devastating. For example, in healthcare, data breaches are estimated to cost an average of $10 million per incident (far above the cross-industry average) when you factor in lost productivity and patient trust. In manufacturing, a single cyber-induced production outage can ripple through supply chains and cause multi-million dollar losses per day. The *global trend data* is unambiguous: breaches are

growing in frequency and scale each year, and more data is being compromised than ever before. In 2023, a record 1,300+ data breaches were reported in the U.S., and 2024 saw even more records exposed due to several mega-breaches in tech and healthcare.

One striking statistic is that 74% of all breaches involve the "human element" – whether through error, phishing, or misuse. This underscores that simply buying tools or drafting policies (the checkbox approach) is insufficient; *human behaviour and culture* are central to security. Many organizations afflicted by breaches had invested in modern security technologies, yet still fell victim because an employee clicked a malicious link or a critical process wasn't followed. Without a culture of vigilance and continual learning, even the best tools can be undone by a single mistake. Attackers are well aware of this and increasingly target people rather than systems. For instance, business email compromise (a social engineering con) has caused billions in fraud losses even at companies that had state-of-the-art network defences. The trend of "shift left" in cyber attacks – going after softer targets like supply chains and end-users – exploits the gaps left by compliance-focused security programs. Those programs often emphasize technical checklists (firewalls, antivirus, encryption of data at rest, etc.) but may not sufficiently address user awareness, third-party vetting, or incident response preparedness.

Another development is the hardening stance of regulators and insurers, which is both a consequence of past failures and a catalyst for change. Government policy trends globally are making cybersecurity a board-level responsibility by mandate. In the European Union, the new NIS2 Directive (effective 2024) explicitly requires that the "management body" (i.e. board and senior executives) of essential entities *approve and oversee cybersecurity measures* and be held personally liable for non-compliance. This is a major shift – cyber can no longer be delegated down to IT departments; it must be treated as a core governance issue. For many EU boardrooms, this is indeed a "cultural shock". In the United States, the SEC in 2023 adopted new rules requiring publicly traded companies to disclose their cybersecurity risk management and governance practices, including how the board oversees cyber risks. While the SEC stopped short of requiring a cyber expert on the board, it compels transparency around whether the board is paying attention – effectively pressuring directors to step up oversight.

Regulators are also shortening the timeline for incident reporting (e.g. SEC mandates disclosure of material breaches within 4 business days), forcing companies to have robust incident response plans at the ready. Meanwhile, cybersecurity insurance providers are tightening their requirements and hiking premiums; many now require evidence of advanced controls (like multifactor authentication, employee training, and even "real-time security telemetry") before granting coverage. Insurers have suffered huge payouts from ransomware incidents and thus are pushing clients towards true security improvements rather than just paperwork. We're even seeing the prospect of legal liability for executives: after major breaches, shareholders and customers have filed lawsuits claiming that leaders breached their duty of care in cybersecurity (for example, derivative suits following the SolarWinds and Colonial Pipeline incidents). All these trends send a clear message: *the era of cybersecurity complacency at the top is ending*. Organizations that treated cyber as a mere compliance item are now facing external consequences, from fines and legal actions to inability to obtain insurance, that make this approach untenable.

In short, the cost of superficial security is no longer confined to technical realms – it is now translating into strategic business risks. Companies that fail to embed cybersecurity into their culture and operations suffer more breaches (with associated costs), lose out competitively (as customers favour secure partners), and risk regulatory punishment. Conversely, those that treat cybersecurity as a first-class business risk are seeing benefits. Studies find that organizations adopting leading security frameworks and a proactive posture have fewer security incidents and even enjoy financial perks like lower cyber insurance premiums. In the next section, we turn to how businesses can achieve this proactive, culture-driven approach to cybersecurity.

It is evident that a fundamental shift is needed: from viewing cybersecurity as a checklist or occasional project, to embracing it as a core component of corporate culture and enterprise risk management. This transformation must start at the top – with boards of directors and C-suite executives – and permeate every level of the organization. Below, we outline strategies and actionable frameworks to integrate cybersecurity into board-level decision-making, everyday business processes, and the organizational mindset. Key themes include leadership accountability, cultural change, cross-departmental collaboration, and long-term planning.

Leadership and Board Responsibility

Creating a strong security culture begins with leadership commitment. Executives and directors must not only support cybersecurity in words, but also model the behaviours and prioritize the actions that demonstrate its importance. A common saying is that the *"tone at the top"* determines whether security initiatives flourish or flounder. Concrete steps for leadership include:

- Make cybersecurity a standing agenda item at board meetings. Boards should receive regular briefings on cyber threats, incidents, and readiness, in plain business terms. Rather than sporadic, jargon-laden updates (a common pitfall), cyber risk should be discussed with the same frequency and rigor as financial or operational risk. This signals that the organization treats security as integral to its mission. It also enables directors to ask probing questions and hold management accountable for improvements. If current board members lack cyber expertise, boards can bring in advisors or arrange training so they "have sufficient knowledge to assess cyber risk," as NIS2 mandates. The goal is informed oversight: directors need to understand the business impact of cyber risks and ensure appropriate resources are allocated.

- Assign clear cybersecurity oversight roles at the board and executive level. Many companies now designate a specific board committee (often an Audit/Risk Committee) to oversee cybersecurity. The SEC's disclosure rule expects companies to state which committee or subcommittee is responsible. What matters most is that *someone* at the board level is explicitly charged with this duty. Similarly, within executive management, the reporting lines for the Chief Information Security Officer (CISO) should enable unfettered communication of risks – ideally the CISO reporting to the CEO or another top executive, rather than being buried several layers down. Some leading organizations have created management-level cyber risk committees that include leaders from IT, finance, legal, operations, and HR, recognizing that cyber risk is multidisciplinary. The board should insist on clarity: who owns cyber risk management and how are they empowered? If that question cannot be answered crisply, it's a red flag.

- Tie cybersecurity to business objectives and KPIs. Leadership should integrate security metrics into the company's performance framework. For instance, a bank might include cybersecurity preparedness as part of its balanced scorecard or link a portion of executive compensation to meeting certain security maturity targets. This moves security from a purely technical realm into business accountability. However, care is needed to choose meaningful metrics (e.g. time to patch critical vulnerabilities, results of phishing tests, etc.) rather than vanity metrics (number of policies written). The board can guide this by demanding metrics that reflect risk reduction and resilience, not just compliance. When leadership visibly cares about these metrics, so will the rest of the organization.

- Lead by example in daily practices. Executives and managers must *personally* follow good security hygiene – using strong passwords (or password managers), adhering to authentication policies, taking security training seriously, and so on. An oft-cited strategy is for leaders to "walk the talk": if rank-and-file employees see the CEO getting phished in an internal drill and shrugging it off, they will mirror that attitude. Conversely, if they see top leaders actively championing secure behaviour (for example, a COO sharing how she enabled multi-factor

authentication on her accounts and encouraging others to do the same), it reinforces that security is everyone's job. Some companies have executives periodically send out notes or videos about current cyber issues (like warning about a new phishing scam), underscoring leadership engagement.

In essence, cybersecurity must be elevated to a core governance issue, not something tacked on or delegated away. As a recent Harvard Business Review article noted, too many boards *"overestimate their company's cybersecurity preparedness"* and are not sufficiently proactive. The remedy is for boards to adopt a stewardship mindset, treating cybersecurity as integral to fiduciary duty. Regulators are increasingly demanding this, as discussed. The EU's approach even threatens personal liability for board members who ignore these obligations. Forward-looking companies aren't waiting for mandates – they are voluntarily bringing cyber risk into the strategic planning conversation.

Ultimately, leadership's message should be: "Compliance is not our goal, security is". This reframes all decisions to ask, "Are we actually safer, or just seemingly compliant?"

Fostering a Security-First Culture

Beyond formal governance, organizations need to embed security awareness and responsibility into their day-to-day culture. A strong cybersecurity culture means employees at all levels "do the right thing, even when no one is watching," to paraphrase one definition. It involves values and norms that encourage vigilance, mutual support, and openness about security. Achieving this requires sustained effort in a few key areas:

Education and continuous awareness: Traditional annual security trainings are notoriously ineffective at changing behaviour. Instead, leading organizations implement ongoing awareness programs that are engaging, frequent, and relevant. This could include monthly phishing simulation exercises with immediate feedback, short "security tip" newsletters, gamified challenges, and internal campaigns around Cybersecurity Awareness Month. The content should evolve with emerging threats (e.g. guidance on work-from-home security, recognizing social engineering ploys, etc.). Importantly, awareness efforts should connect security to employees' personal and professional lives – *why* it matters. For example, a hospital might emphasize that clicking a malicious link could down systems and impact patient care, making the risk tangible to staff. Positive reinforcement helps too: celebrating teams with the best security quiz scores or individuals who report phishing attempts can make security a shared point of pride. According to research, organizations with a strong security culture are over five times more likely to have good security practices across the board. This is not achieved overnight; it's the result of persistent messaging and leadership reinforcement.

Integrate cybersecurity into onboarding and regular communications: New employees should learn about the company's security values from day one. Many firms now include a security briefing in orientation, not just as a checklist but to instill the idea that "this is how we work here." Likewise, managers can incorporate security topics into team meetings when relevant (for instance, a department head might remind everyone about a new policy for data classification and handling). The goal is to weave security into the fabric of operations, rather than treating it as an external add-on. Some companies have found success by identifying *security champions* within departments – regular staff who get extra training and act as liaisons to IT/security teams. These champions help spread good practices and act as local eyes and ears for security issues, creating a grassroots support network.

Encourage a no-blame reporting culture: One cultural aspect that can significantly improve security is removing fear around reporting potential security incidents or mistakes. Employees should feel safe to say "I clicked something suspicious" or "I think I lost a company device" immediately, rather than concealing it out of worry they'll be punished. Leadership should promote the message that *reporting early is always the right move*, and response will focus on fixing the problem, not blaming the individual. This approach is borrowed from safety cultures in industries like aviation and healthcare, where incident reporting is crucial for prevention. It can be reinforced by policies (e.g. amnesty for self-reported clicks during phishing tests, up to a point) and by managers' reactions. When an issue is reported, thanking the person and responding constructively encourages others to come forward. If issues are swept under the rug, small problems can metastasize into breaches. A transparent, blame-free culture also means conducting honest post-incident reviews and sharing lessons learned internally, rather than hiding failures.

Align security with mission and values: People are more likely to embrace security if they see it as supporting the organization's mission, not hindering it. For instance, at a fintech company, developers can be made to feel that building

secure software is part of innovating with integrity. At a university, faculty and students might be reminded that good security enables academic freedom by protecting intellectual property and personal privacy. Many organizations have started to articulate cybersecurity principles as extensions of their core values (e.g. trust, quality, safety). By framing it this way, security stops being "the Department of No" and becomes a positive attribute of the company's identity.

Leaders have to actively drive this cultural shift. As one CEO described, you need leaders willing to *"invest the time into cybersecurity culture"* and embed security into every business process, because the CISO alone "can't be everywhere at once". This means that in each domain – whether it's finance, HR, manufacturing, or IT – managers take ownership of the cyber risks in their area, guided by the central security team. For example, the head of HR ensures that background checks and least-privilege access for new hires are in place; the head of product development builds secure design reviews into the development lifecycle. When leadership in each department cares about security, it stops being an external pressure and becomes a normal part of "how we do things around here."

Cross-Departmental Integration and Collaboration

Cybersecurity can no longer be confined to an IT silo. Effective defence and resilience require cross-functional integration. This is because cyber risk intersects with many parts of the business: legal (compliance and breach liability), finance (budgeting and insurance), operations (maintaining uptime), HR (people and training), procurement (supply chain security), and so forth. A few practical frameworks and actions can facilitate this integration:

- Enterprise Risk Management (ERM) framework: Organizations should include cyber risks in their overall ERM program, alongside financial, operational, and strategic risks. This involves identifying key cyber risk scenarios (e.g. "major data breach of customer info" or "ransomware disrupts production for 1 week") and analyzing their potential impact in business terms. By doing so, cybersecurity moves into the language executives understand – risk appetite, likelihood, impact, mitigation strategies. Many companies use risk registers and heat maps to compare cyber risks with others. This helps in prioritizing investments: e.g., if "loss of sensitive customer data" is one of the top enterprise risks, the company might decide to invest in encryption, data loss prevention, and zero-trust access controls as strategic initiatives. Boards and audit committees increasingly expect to see cyber risk treated in this holistic way. Integrating it into ERM also encourages different functions to collaborate on risk mitigation (for instance, IT working with legal on data privacy controls, or with operations on incident response plans).

- Incident response and business continuity planning: Cyber incidents often demand a coordinated response across departments – technical containment by IT, customer communications by PR, legal notifications for regulators, insurance claims handling, etc. Developing and exercising incident response plans with cross-department participation is crucial. Tabletop simulations at the executive level can surface gaps and build muscle memory. One common failing noted in breaches is "fragmented or overly complicated incident plans" that omit clear roles and escalation paths. Simplifying and unifying these plans is important. For example, the plan should clearly define when an incident requires invoking the crisis management team, who needs to be informed immediately, and who has decision authority (e.g. on shutting down systems, paying ransom or not, public disclosure, etc.). Cross-functional drills ensure that, in a real event, the organization responds as a cohesive unit, not in silos that cause delay and confusion. As NIS2 and other regulations impose strict reporting timelines (some EU countries will have as short as 24 hours to report certain incidents), being well-rehearsed is not optional. The NHS's WannaCry experience, where lack of a tested plan led to ad hoc chaos, is a cautionary tale; contrast that with firms who had practiced and therefore managed a swift, composed response to incidents.

- Integrating security into project lifecycles: Whether it's deploying a new IT system, launching a new product, or onboarding a new vendor, security should be a built-in checkpoint in the process. Many organizations now embrace DevSecOps in software development – embedding security testing and code review into the CI/CD pipeline, so vulnerabilities are caught early. Likewise, procurement processes are evolving to include vendor security assessments as a standard step (with automation tools helping to streamline this). The idea is that security is not a separate hurdle at the end, but a thread woven through every stage. This reduces friction in the long run, as fewer "surprises" crop up right before go-live, and teams internalize security considerations as part of their normal work. Cross-department collaboration is needed here: IT/security teams should partner with business units to develop security criteria that align with business needs (for example, a marketing team

choosing a cloud SaaS tool should have a checklist of security/privacy features to look for, provided by the security team).

- Information sharing and external collaboration: No organization can tackle cyber threats alone. A culture that embraces sharing threat information and best practices with peers (through industry ISACs – Information Sharing and Analysis Centres – or informal networks) will be more resilient. For example, financial services have FS-ISAC, healthcare has its H-ISAC, etc., where companies circulate intelligence about emerging threats. Internally, teams should also share information rather than hoard it – IT operations and security, for instance, must work hand in hand (one positive trend is the rise of unified SecOps centres). Breaking down silos between teams like network admins, application developers, and security analysts leads to quicker detection and remediation. Some companies co-locate these teams or use collaborative platforms to ensure everyone has the same visibility. The cultural message is "we're all in this together" against cyber threats.

The common thread in all effective integration efforts is the recognition that cybersecurity is no longer the exclusive domain of the IT department – it becomes everybody's business. Security must be viewed not as an isolated function, but as a shared responsibility that touches every department, every role, and every process within an organization. This shift in mindset is critical, especially as cyber threats increasingly exploit non-technical vulnerabilities, including employee behaviour, supply chain partners, and operational blind spots.

As highlighted in the KPMG/MIT Cybersecurity Culture study, a resilient cybersecurity posture depends heavily on culture – and that culture must be "holistic across an organization, extending from individual level to the full ecosystem of the business and its suppliers." In other words, cybersecurity excellence is not achieved solely by technical controls or policy documents, but by the collective vigilance and commitment of people at every level, from the boardroom to the back office.
Leaders are central to making this a reality. They drive cultural alignment by embedding security principles into managerial mechanisms that shape everyday behaviour and strategic decision-making. This includes incorporating cybersecurity metrics into performance evaluations, so that individuals and teams are held accountable for secure practices. It involves recognition and incentive programs that actively reward positive security behaviour – such as reporting phishing attempts, adhering to best practices, or contributing to threat awareness campaigns – thereby reinforcing the idea that good cybersecurity is both visible and valued.

Governance structures play a key role as well. When cybersecurity is represented within risk committees, strategy groups, and cross-functional working teams, it gains the visibility and authority it needs to be embedded across the organization. This ensures that cyber considerations inform decisions not only in IT and compliance, but in areas like procurement, product development, HR, and legal.

When these efforts are sustained and thoughtfully executed, cybersecurity becomes second nature, woven into processes just like quality assurance or workplace safety became in previous industrial eras. Just as manufacturers now routinely embed safety checks into every stage of production, forward-thinking organizations are building cybersecurity checkpoints into everything from onboarding and vendor selection to software deployment and customer engagement. Over time, this operationalises security as a cultural norm – not an exception, not a burden, but a basic expectation.
In doing so, the organization shifts from a reactive, rule-based posture to a proactive, risk-aware environment where everyone plays a role in reducing exposure and increasing resilience.

This is the essence of a true security culture: not just rules or awareness campaigns, but a deeply held organisational belief that protecting data, systems, and trust is part of every job.

Finally, moving from a reactive, compliance-oriented posture to a proactive, culture-driven one requires adopting long-term planning and recognized frameworks to guide the journey. Compliance tends to focus on short-term tasks (pass this year's audit); in contrast, a strategic approach involves setting multi-year maturity goals and continuously improving. Here are key aspects:

Adopt and tailor industry frameworks: Frameworks like the NIST Cybersecurity Framework (CSF), ISO 27001, or others provide a comprehensive map of security domains and controls. They are valuable for ensuring no major area is overlooked (governance, asset management, detection, response, recovery, etc. all get covered). Importantly, these frameworks encourage a risk-based approach – implementing controls commensurate with risk. By adopting a framework as a *guide*, organizations can move beyond mere compliance with one regulation and instead aim for a more robust posture. For instance, a healthcare entity that embraces NIST CSF 2.0 may find that it addresses HIPAA requirements as a byproduct, but goes further to address emerging issues like medical device security and supply chain risk which HIPAA doesn't explicitly cover. Studies have shown that organizations adhering to leading frameworks shift from reactive to proactive security, resulting in fewer breaches. Moreover, companies that leverage frameworks like NIST often gain measurable benefits like reduced incident costs and more favourable insurance terms. The key is not just to adopt a framework on paper, but to actively use it in planning and assessments. Frameworks can serve as a common language between technical and non-technical stakeholders (e.g., a board dashboard might be organized around NIST's five functions: Identify, Protect, Detect, Respond, Recover, giving high-level insight into each). As with any guide, it should be tailored to the organization's context; for example, a manufacturing firm might emphasize physical/OT security controls, whereas a cloud-based software company focuses on application and data security.

Maturity road mapping: Achieving cultural and security maturity is a multi-year effort. Organizations should assess their current state (possibly via a cybersecurity maturity assessment tool or external audit) and define a target state – then lay out a roadmap with concrete milestones. This might include projects like deploying an enterprise-wide identity management system this year, instituting 24/7 security monitoring next year, steadily improving patch management timeframes, and so on. Each milestone should have ownership and resources attached. By visualizing the journey, leadership can allocate budget and track progress more effectively, rather than endless reactive spending with no clear plan. Maturity models like CMMI for Security or the Cybersecurity Capability Maturity Model (C2M2) can be useful benchmarks. Some regulators now expect to see such roadmaps; for instance, U.S. financial regulators often ask for a 3-5 year cyber strategy during exams. A maturity approach also helps avoid complacency – even if you're compliant today, you recognize there's a next level of capability to reach tomorrow.

Investment in people and skills: Long-term planning must factor in the human element. This means not only continuous training for all employees (as discussed) but also developing cybersecurity talent internally and recruiting where necessary. Many organizations struggle to fill skilled security roles; one solution is to create rotation programs or upskilling initiatives for IT staff to become security specialists. Another aspect is giving the security team a prominent voice and backing within the organization. It has been noted that true cybersecurity professionals may leave if they're treated as mere checklist operators. To retain and empower talent, companies should build a culture where security expertise is valued – involving security personnel in business discussions, heeding their counsel, and providing them growth opportunities. Some companies are establishing cyber labs or centres of excellence internally to focus on innovation (like using AI for threat detection) and to keep talent engaged in advancing the state of the art. A long-term outlook on staffing and culture recognizes that technology alone doesn't solve security – people do.

Monitoring and adapting: A secure culture is not a one-and-done achievement; it requires monitoring and adaptation. Organizations should use metrics and audits not just for compliance, but to gauge cultural penetration. For example, annual surveys on cybersecurity culture can be conducted to understand employee attitudes and areas of weakness. The results might highlight, say, that employees in a certain region or department feel disengaged from security – prompting targeted interventions. Some advanced programs quantify culture (using tools like the "Security Culture Framework"

surveys) and set goals to improve it year over year. Additionally, threat environments change, so long-term plans should be revisited at least annually to adjust priorities. The emergence of new threats like AI-driven attacks or changes in the business (e.g. a big move to cloud services) may necessitate re-scoping the strategy. Agile governance processes that can reallocate resources when needed are crucial. The board and executives should stay informed through continuing education on cyber trends – many boards now invite outside experts for periodic briefings or attend cyber risk workshops as part of their development.

Ultimately, transitioning to a culture-embedded, strategy-driven approach to cybersecurity is not a quick fix – it is a long-term transformation that may take years to fully embed across all levels of an organization. It requires sustained commitment, cross-functional alignment, and a willingness to rethink long-held assumptions about where cyber risk resides and who is responsible for managing it. Despite the effort involved, this shift has become not just important, but imperative for long-term resilience and business continuity.

The outdated mindset that equates "security" with "compliance" must be actively dismantled. While compliance can provide a useful baseline, it is not a guarantee of protection – and treating it as such leaves organizations dangerously exposed. As one cybersecurity leader aptly observed, "Compliance without competence is negligence." That negligence, once an internal liability, has now evolved into a strategic vulnerability that can lead to operational collapse, regulatory penalties, shareholder lawsuits, and lasting reputational damage. In today's threat environment, the cost of getting cybersecurity wrong is higher than ever, and ignorance is no longer an excuse.

Conversely, organizations that successfully foster a strong security culture and embed it into their core operations often find that it becomes a powerful competitive advantage. These businesses are better equipped to detect and respond to emerging threats, maintain operational continuity during cyber incidents, and recover quickly when disruptions do occur. Perhaps more importantly, they project confidence to customers, partners, and regulators – demonstrating that they take data protection, privacy, and trust seriously. In markets where consumers and clients increasingly demand accountability, transparency, and assurance, a visibly strong cybersecurity posture can be a key differentiator.

Embedding cybersecurity at the board level and throughout the organizational fabric is, in essence, an act of future-proofing the business. It means aligning security with growth, innovation, and governance, rather than treating it as a constraint. It ensures that as the digital risk landscape evolves – with new technologies, attack vectors, and regulatory pressures – the business is prepared not only to survive, but to thrive.

In a world where cyber threats are constant and trust is fragile, companies that treat cybersecurity as a foundational value, rather than a compliance afterthought, are the ones most likely to endure. The journey is complex, but the payoff is resilience, credibility, and long-term strategic advantage.

The persistent failure of cybersecurity efforts globally – across industries and nations – reveals a fundamental lesson: security cannot succeed as an afterthought or a formality. Treating cybersecurity as a mere compliance checkbox, rather than a core organizational value, is a recipe for disaster. We have seen how companies that boast compliance certifications or pass audits have nonetheless fallen victim to devastating breaches. The missing ingredient was not a lack of rules or technologies, but a lack of security-minded culture and leadership. From Equifax's complacency to Target's narrow focus, from the NHS's top-level inaction to Maersk's pre-NotPetya laxity, the common thread is clear. In too many cases, corporate leaders signalled "we're secure" on paper while tolerating serious vulnerabilities in practice. As the saying goes, *"Businesses fail when leaders mistake movement for progress"*. Cybersecurity has often been full of movement – policies written, tools installed, compliance reports filed – but lacking in genuine progress towards resilience.

Changing this trajectory requires a collective commitment to embed cybersecurity into the fabric of how organizations operate. It means leadership championing cyber risk as equal in importance to financial, legal, or any other strategic risk. It means cultivating a workforce where every individual understands their role in protecting the enterprise, and feels accountable for it. It means breaking down silos so that security considerations inform all business decisions, from product design to vendor selection. And it means planning for the long haul – anticipating how to adapt as the threat landscape evolves, rather than reacting in crisis mode. None of this is easy, but the alternative – continuing with superficial checkbox security – is far worse. The future will not be kind to organizations that persist in seeing cybersecurity as a cost center annoyance or a trophy compliance project.

Fortunately, we see positive momentum. Governments and regulators are pushing boards to take responsibility, experts and industry groups are providing roadmaps for cultural transformation, and many forward-thinking companies are already reaping the benefits of a security-first ethos. Executives are coming to recognize that cybersecurity is not just an IT issue, but a business enabler and a trust cornerstone. As this realization spreads, we can be guardedly optimistic that the historical cycle of cyber failures can be broken. Success will be measured not by absence of incidents (some attacks will inevitably get through), but by how well organizations prevent what they can and handle what they cannot, minimizing damage and bouncing back stronger.

An enterprise with security in its culture will detect threats sooner, respond more effectively, and learn continuously, thereby thwarting many attacks and reducing the impact of the rest. In sum, embedding cybersecurity into culture and strategy is the way we align our defences with the realities of a digital world, turning a systemic weakness into a sustainable strength.

About CAGI

The Cybersecurity & Artificial Intelligence Governance Initiative (CAGI) is an independent, international institute focused on closing the gap between rapidly evolving technologies and effective governance.

CAGI brings together industry leaders, practitioners, academics, and public-sector stakeholders to translate foresight into actionable governance. The institute operates as a neutral platform, providing evidence-based guidance rather than advocacy or compliance checklists.

Get involved: CAGI welcomes participation from individual professionals, corporate members, and sponsors who wish to contribute to the development of credible, future-ready governance and to help shape how AI and cybersecurity are governed in practice - www.thecagi.com

Sources:

- Barsky, N.P. & Pearlson, K. (2025). *Boards Need a More Active Approach to Cybersecurity*. Harvard Business Review – survey of executives on board cyber oversight.
- CardConnect. (2017). *What We Learned from Target's Data Breach 2013* – Case study on PCI compliance vs. Target breach.
- Johnson, D.B. (2018). *'Culture of cybersecurity complacency' blamed for 2017 Equifax hack*. Nextgov – U.S. House Oversight Committee report findings.
- Alder, S. (2025). *Healthcare Cybersecurity Benchmarking Study 2025*. HIPAA Journal – finding that adopting frameworks (NIST CSF) yields fewer breaches.
- Boiten, E. & Wall, D. (2017). *WannaCry report shows NHS chiefs knew of danger, but management took no action*. Scientific American / NAO Report – analysis of NHS WannaCry failings.
- Sipmann, K. (2025). *The Illusion of Compliance: Why Cybersecurity Theater is Setting the Stage for Catastrophic Failure*. Medium – expert commentary on compliance vs. security mindset.
- KPMG & MIT Sloan CAMS. (2024). *A new age of cybersecurity culture* – research on cybersecurity culture and leadership.
- Advisense. (2025). *NIS2: When the Board Becomes the Weakest Link* – discussion of EU NIS2 directive and board responsibilities.
- KPMG Board Leadership Center. (2023). *SEC's final cybersecurity rules: A board lens* – summary of SEC disclosure requirements for cyber risk governance.
- Digital Guardian. (2018). *Lack of Knowledge, Visibility Contributed to Equifax Breach* – highlights Equifax issues like unpatched vulns and expired certs.
- Greenberg, A. (2018). *The Untold Story of NotPetya…* WIRED – impact of NotPetya on Maersk and global firms.
- ComputerWeekly. (2019). *NotPetya offers industry-wide lessons, says Maersk's tech chief* – insights from Maersk CTO on attack and response.
- HIPAA Journal. (2025). *Healthcare Data Breach Statistics* – record breaches and records exposed in 2023.
- Secureframe. (2025). *110+ Latest Data Breach Statistics [2025]* – global cybercrime cost and breach trends.