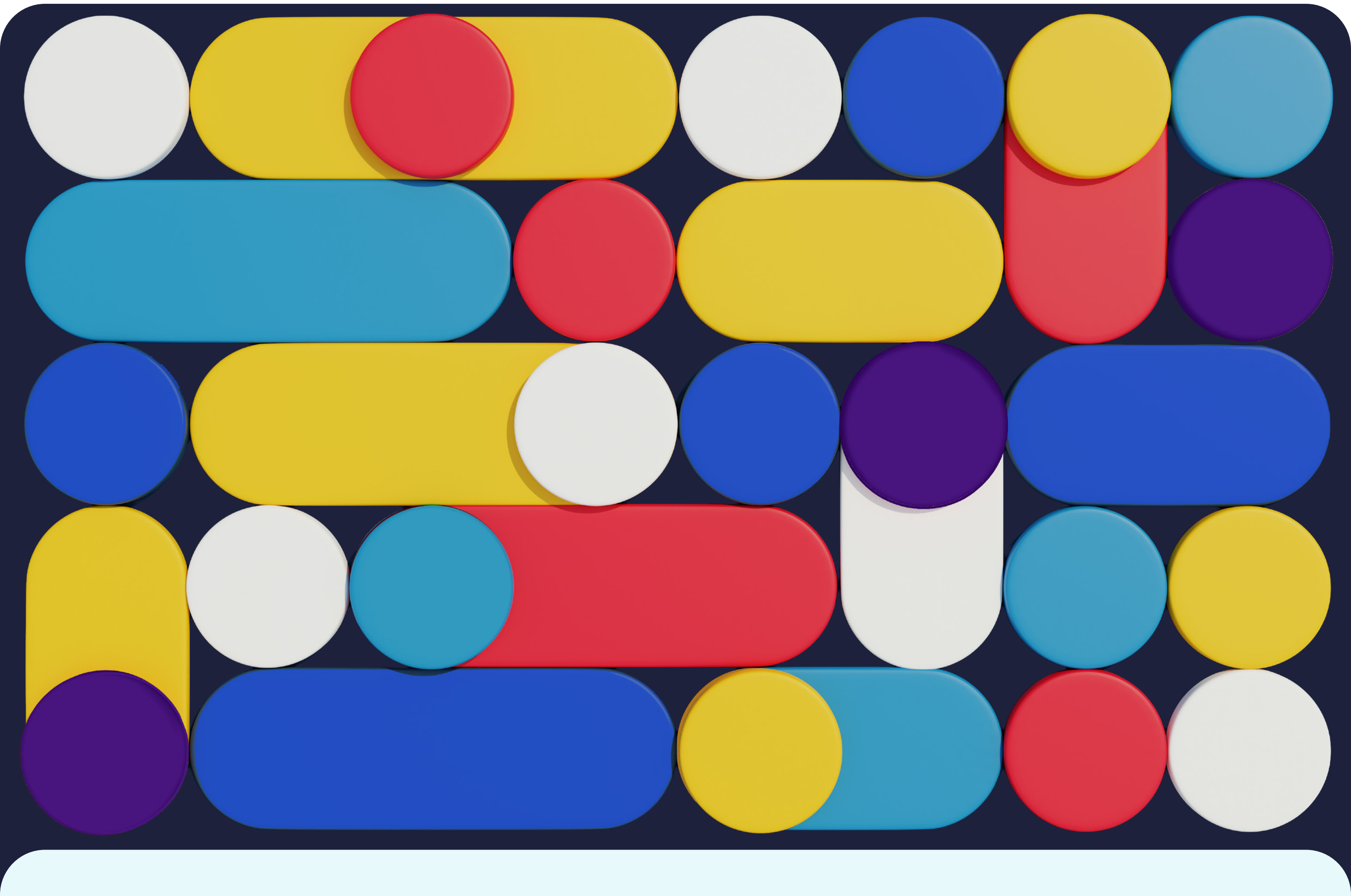
PROTECHT



E-BOOK

Too many cyber tools, not enough truth – and what to do about it.

When it comes to cyber, most organisations aren't short of controls; they're short of proof. Tool sprawl and overlapping frameworks scatter evidence and blur ownership, so when incidents hit, response becomes a scramble for facts across teams and suppliers. The answer isn't more complexity. It's connected, provable resilience.

Executive summary.

Cyber has become a chronic condition

Cyber risk no longer behaves like a security problem you can contain within IT. It behaves more like a chronic condition: recurring, cross-functional and increasingly public.

Cyber crime risk by the numbers:

Average days to identify a cyber breach

200+

(IBM[1])

Increase in attack events for the average enterprise

44%

(Check Point[2])

Average days enterprise cyber security stack

45 tools

(Gartner[3])

Increase in cyber intrusions coming from China

150%

(CrowdStrike[4])

Disruption is now the headline outcome

Cyber harm is rising beyond data theft into disruption. Ransomware remains pervasive. Phishing is still the workhorse. Vulnerability exploitation rewards speed. Attackers do not need genius; they need scale and they exploit the ordinary: misconfigurations, reused credentials, delayed patching, and confused handoffs.

The old incident story no longer fits

The 'breach, clean-up, move on' model of old doesn't match present day reality. Even when recovery is fast, the consequences are real and can continue to multiply: services stall, decisions pause, customers notice, and explanations are demanded while the facts are still moving.

Fragmentation is the quiet force multiplier

Too many tools. Too many frameworks. Too many versions of the same control. Under pressure, assurance becomes an exercise in stitching together screenshots, spreadsheets and partial truths, precisely when speed and credibility matter most.

AI accelerates loss of control

Attackers use AI to scale. Employees use AI to move faster. Gartner flags two emerging risks that will feel familiar to anyone who has lived through fragmentation: Shadow AI and information-governance-driven AI risk, where sensitive data drifts into tools nobody approved, or into models fed by weak governance.[4]

The new centre of gravity is provable resilience

Cyber is no longer about preventing every incident. It is about continuity, control and confidence, and about being able to prove them when the clock is running.

[1] Cost of a Data Breach Report, IBM.
[2] Cyber Security Report 2025, Check Point.
[3] Gartner: Q3 25 Emerging Risks report.
[4] Global Threat Report 2025, CrowdStrike.

Contents.

1 The cyber problem has changed.

Cyber risk is no longer defined by the occasional breach. It is defined by volume, impact and speed. What used to be treated as an IT failure is now a continuous business risk: one that tests continuity, leadership confidence and regulatory assurance at the same time.

The scale has shifted

Cyber crime is rising, with the average organisation facing a 44% increase in the number of attempted cyber attacks in 2024.[5] Although it's hard to determine a financial value, various credible estimates put the economic impact of cyber crime above US$1 trillion in 2025.[6] According to IBM's Cost of a Data Breach Report, breach identification and containment takes the best part of a year. As IBM notes, "*the longer a breach goes undetected, the more costly it becomes*".[7]

But scale is only the starting point. What has really changed is how cyber incidents behave once they begin. Detection and response are no longer discrete phases; they are a prolonged drain on time, money and attention.

> Cyber incidents are no longer an exception. They are a steady condition of operating.
>
> ~ **Michael Franklin**,
> Cyber Security Lead, Protecht

The accountability clock is now public

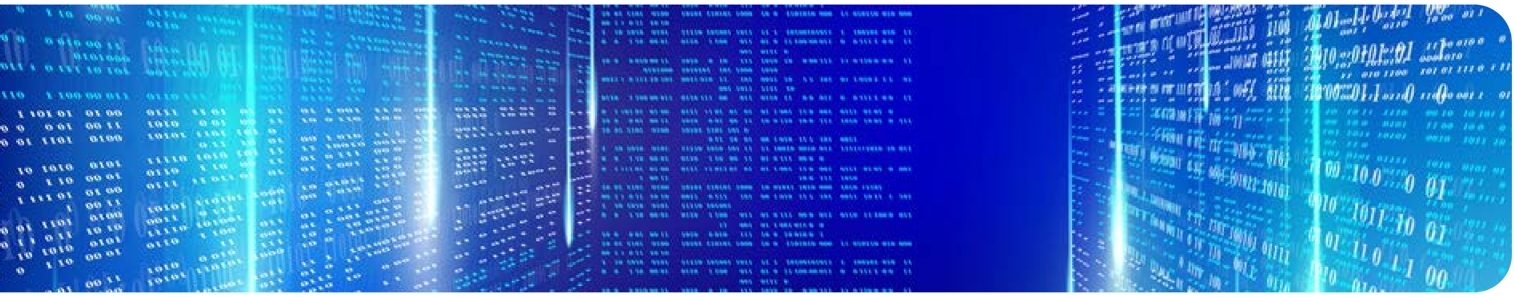
Expectations around disclosure are tightening. The US SEC requires material cyber incidents to be disclosed within four business days, while European and Australian regimes impose similarly compressed timelines.[8] The implication is stark: organisations are expected to explain what happened, and what still works, before they have fully stabilised the situation.

Verizon's DBIR reinforces the pressure: incidents are increasingly frequent and overlapping, not isolated one-offs.[9] Confidence can no longer be asserted after the fact. It must be demonstrated, under pressure, with evidence.

The next shift is already here: AI

In addition to the increased use of AI-based tools to drive cyber-attacks, Gartner's emerging-risk research flags **shadow AI** and **information-governance-driven AI risk** as rising concerns, because the fastest way to lose control is often letting sensitive data drift into tools nobody approved.[10]

This is the new cyber reality. The defining question is no longer whether incidents will occur, but whether organisations can demonstrate continuity, control and confidence when they do.



[5] Cyber Security Report 2025, Check Point.
[6] The True Cost of Cybercrime, Cyber Defense.
[7] Cost of a Data Breach Report, IBM.
[8] Cyber incident disclosure SEC.
[9] Data Breach Investigations Report Verizon.
[10] 2025 Q3 Emerging Risks, Gartner.

Case example: AWS US-East-1 outage – when cyber isn't the failure

A configuration issue at Amazon Web Services' US-East-1 region disrupted access to dozens of downstream services, including major airlines, financial platforms and consumer applications.[11]

There was no breach, no malware, and no data theft, yet customer services stalled, internal operations halted, and public explanations were demanded immediately.

For affected organisations, the challenge was not stopping an attack. It was proving resilience in the face of sudden dependency failure.

The lesson:

Severe disruption does not require a threat actor. In a tightly interconnected digital ecosystem, operational resilience must extend beyond cyber defence to managing concentration risk and critical service dependencies.

[11] AWS: Amazon.

2 Cyber harm is rising beyond IT.

Cyber incidents are no longer occasional 'IT events'. They are business-disruption campaigns: persistent, opportunistic and increasingly fast.

The FBI's Internet Crime Complaint Center (IC3) calls ransomware "again the most pervasive threat to critical infrastructure". In 2024 it logged 3,156 ransomware complaints, up 9% year on year.[12] Ransomware is not just about stolen data. It is about denied access, stalled operations and a clock that keeps ticking while everyone argues over what happened.

The entry point is rarely exotic. ENISA's latest threat landscape for Europe is blunt:

> Phishing remains the dominant intrusion vector (60%).[13]

That is not a triumph of genius so much as a triumph of scale. Industrialised, AI-enabled 'phishing-as-a-service' means one attacker can run dozens of campaigns while your staff are still hunting for the right mailbox rule.

When phishing fails, attackers go shopping for weakness elsewhere. ENISA also notes:

> Vulnerability exploitation remains a cornerstone of initial access (21.3&), underscoring the need to ensure patch availability.

The uncomfortable catch is that patch availability is not the same as patch safety. Patching takes planning; exploitation takes minutes.

The time-compressed reality:

- Mandiant found that, among zero-day vulnerabilities it tracked in 2023, "12%... were exploited within one day" of a patch being available, and 29% within a week.[14]
- In other words: the warning window is often shorter than a weekly change-control meeting.

Case example: MOVEit – one flaw, many victims

Progress Software's MOVEit Transfer (a managed file-transfer tool) was hit by a zero-day (CVE-2023-34362) exploited for data theft.

CISA and the FBI said they were "aware of exploitation... beginning in late May 2023".[15] Mandiant reports "the earliest evidence of exploitation occurred on May 27, 2023", followed by web shells and rapid theft.

The lesson:

The episode mattered because it showed how quickly a niche system can become a mass event: not through better hackers, but through better timing.

[12] Internet Crime Report 2024, IC3.
[13] Threat Landscape 2025, ENISA.
[14] Mandiant, Google Cloud.
[15] CISA advisory AA23-158A, CISA.

3 The new stakes: continuity, trust, operational resilience.

The next big disruption may not arrive with a ransom note. It may arrive as a supplier failure, a routine update that misfires, or an internal change that ricochets through your stack. The screens go blue, the service desk lights up, and the executive team still asks the same question: are we still operating and can we prove it?

From breach to business disruption

The impact is increasingly business-shaped, even when the trigger is technical. As we've seen earlier, IBM's data shows that breaches last long enough for disruption to become a management problem, not just an IT one.

But disruption does not need a sophisticated adversary to hurt. The UK government's Cyber Security Breaches Survey (2025) shows that among organisations that identified a breach or attack, one in six (16%) reported a negative outcome. Specific impacts include temporary loss of access to files or networks (7% of businesses) and loss of access to third-party services (3% of businesses; 5% of charities).[16]

And here's the paradox: even when recovery is fast, the consequences can still be real. For their most disruptive breach or attack, 92% of businesses said operations were back within 24 hours and 77% said it took "no time at all". That does not mean the incident was trivial. It often means the organisation got lucky, or absorbed the pain elsewhere: postponed workflows, delayed decisions, and hurried reassurance.

Trust becomes fragile

In the qualitative interviews behind that same UK survey, one respondent captured the mood:

> The world's changing and it's getting harder to control the risk… on cybersecurity.
>
> ~ **Respondent**,
> UK Cyber Security Breaches Survey

That is not melodrama. It is a description of a trust environment where customers, boards and regulators expect competence at speed and where even a short interruption can turn into a reputational story.

Case example: CrowdStrike's outage – continuity is the new frontline

What happened: CrowdStrike says a content configuration update "resulted in a system crash".

What it wasn't: Their RCA notes the bug was "not exploitable by a threat actor".

Why it matters: CISA described a widespread IT outage stemming from the update: exactly the sort of third-party dependency shock that forces rapid coordination, evidence collection, and board-ready explanation.[17]

The lesson:

The uncomfortable but necessary lesson is that resilience is not only about stopping attackers. It is about designing systems, governance, and response capabilities for the day a trusted control or critical vendor fails.

The new stakes are continuity you can credibly explain and confidence you can credibly defend: staying up, recovering fast, and being able to show clearly, calmly, and with evidence what happened and what still works.

[16] UK Cyber Security Breaches Survey, GOV.UK.
[17] CISA alert on CrowdStrike outage, CISA.gov.

4 Fragmentation: the hidden force multiplier.

Cyber incidents rarely stem from a lack of controls. They stem from lack of visibility into whether those controls are actually effective.

In theory, 'cyber' is one problem. In practice, it is dozens of separate tools, each with its own dashboard, its own data model, and its own opinion of what happened. Gartner's 2024 survey of large enterprises found an average of 45 cybersecurity tools in play drawn from a market of 3,000+ vendors.[18] That is not defence-in-depth. It is decision-fatigue.

Gartner's emerging-risk work has identified an additional fragmentation issue. They define shadow AI as when employees use unauthorised AI tools outside the approved framework, creating data leakage, compliance drift and new, unmonitored entry points.[19]

Then comes the standards pile-up. A US survey by Tenable found 44% of organisations using more than one security framework.[20] Frameworks are useful, but when the same controls are re-tested, re-mapped and re-worded for each regime, 'assurance' turns into admin.

And the glue holding all this together? Often, it is still a spreadsheet. A Compliance Week benchmark survey reported 55% of companies using spreadsheets to monitor regulatory changes; one line in the report puts it bluntly: "most organizations still monitor regulatory changes manually through spreadsheets".[21]

Fragmentation indicators:

- Your tool set is larger than your ability to keep it tuned.
- One control is 'compliant' in one framework and 'missing' in another.
- Your incident narrative depends on who updated the spreadsheet last.
- Third-party evidence arrives late, incomplete or in a different format.

Fragmentation multiplies harm because it slows the only thing that matters under pressure: convergence on facts. Supply-chain incidents make this worse. IBM's 2025 Cost of a Data Breach study found supply-chain compromise involved in 15% of breaches.[22]

When a third party is in the chain, the incident stops being a single investigation and becomes a coordination test. You are no longer just hunting for indicators of compromise. You are chasing timelines, permissions and evidence across multiple owners.

It also changes what 'speed' means. You may need to brief executives, reassure customers, and respond to regulators before you have a stable narrative, because the narrative depends on pieces of evidence that live in different places, under different controls, even under different organisations.

To see how quickly cyber becomes everyone's problem, consider what happened at a large UK university in 2023.

[18] Newsroom, Gartner.
[19] 2025 Q3 Emerging Risks, Gartner.
[20] Trends in Security Framework Adoption, Tenable.
[21] Riskonnect/Compliance Week survey, Riskonnect.
[22] Cost of a Data Breach Report, IBM.

Case example: University of Manchester – one incident, many owners

On 9 June 2023, the University of Manchester, UK reported a cyber incident, saying systems had been accessed by an unauthorised party and data had likely been copied.

The lesson:

The practical response immediately spread beyond the security team:[23]

- The university issued account/password guidance and operational updates for staff and students.
- It published specific instructions for VPN/remote access and other services.
- It said it was working with external agencies including the NCSC and ICO.

In complex organisations, ownership is distributed by design. During an incident that distribution becomes the problem, unless controls, evidence and communication are already joined up.

[23] Cyber update, University of Manchester.

5 What 'good' looks like: provable assurance.

Breaches will happen. 'Good' is what happens next and whether you can prove it.

Perfection is an expensive myth in cyber. Real resilience is more prosaic: a tested response, clear ownership, repeatable reporting, and evidence on demand. When regulators, auditors and your board ask 'what happened?', they are no longer asking for reassurance. They are asking for proof.

The stopwatch has entered the boardroom. Disclosure deadlines are turning cyber incidents into reporting races.

- **United States (SEC):** public companies must file a Form 8-K "within four business days" of determining a cyber incident is material.[24]
- **EU (GDPR):** organisations must notify a supervisory authority "not later than 72 hours" after becoming aware of a personal data breach (unless it's unlikely to result in risk).[25]
- **EU (NIS 2):** "significant incidents" require staged reporting: within 24 hours (early warning), then within 72 hours (incident notification), and a final report within one month.[26]
- **Australia:** Critical infrastructure organisations caught by the SOCI Act must report a critical cyber security incident to the Australian Cyber Security Centre within 12 hours of becoming aware of it (and within
  72 hours for other reportable cyber incidents).[27] APRA-regulated entities must notify APRA of a material information security incident "as soon as possible and, in any case, no later than 72 hours" after becoming aware.[28]

The implication is blunt: if your evidence is scattered, your narrative will be too.

What 'good' looks like in practice:

- Tested response means you can run the playbook under stress, not just admire it in a slide deck.
- Clear ownership means every critical control has a name beside it, not a team, not a committee.
- Repeatable reporting means you can produce consistent answers every time, even when the questions change.
- Evidence on demand means artefacts are retrievable in hours, not chased for weeks.

If this sounds abstract, it's worth looking at what happens when resilience is treated as something you practise, not merely document.

Case example: DeliverEx (Australia) – proof under pressure

The Australian Signals Directorate's Australian Cyber Security Centre describes DeliverEx as "a joint national exercise series that tested the cyber incident response" involving over 60 organisations and 149 participants.[29]

DeliverEx is useful because it treats cyber incidents as they increasingly occur: as multi-organisation events. The value is not the scenario itself; it's what the exercise forces into the open, such as decision rights, information-sharing, regulator-ready reporting workflows, and evidence capture while the facts are still shifting.

The lesson:

It tests whether you can coordinate, document and explain at speed, not just whether you can patch and contain.

[24] SEC resources, SEC.
[25] GDPR, EUR-LEX.
[26] NIS2 staging, EUR-LEX.
[27] Cyber Security Incident Reporting, CISC.
[28] CPS 234 standard, APRA.
[29] DeliverEx, Cyber.gov.au.

6 Connect what matters, cut duplication.

If we know what 'good' looks like, why do so many organisations struggle to get there?

Cyber risk management rarely fails because nobody bought the right tool. It fails because nobody can join the dots fast enough.

Gartner notes that large enterprises now run an average of 45 cybersecurity tools[30], a stack big enough to impress procurement and confuse everyone else. The result is predictable: the same control gets rebuilt, re-tested and re-explained in different places, by different teams, for different audiences.

> By focusing on more tactical, demonstrably beneficial improvements, they can minimise the risks... and more easily demonstrate progress.
>
> ~ **Alex Michaels**,
> Gartner (quoted in Cyber Magazine[31])

Gartner also flags information-governance-driven AI risks: weak governance can feed unintended data into models, producing inaccurate outputs and triggering legal, policy or privacy failures. These are exactly the sort of risk that only joined-up lineage and ownership can contain.

Duplication isn't just wasted effort; it is where assurance goes to die. Tenable found that 44% of organisations use more than one security framework. And 62% said that mapping controls across frameworks creates overlap and duplicate work.[32] That is the quiet tax of modern compliance: endless translation between the same controls expressed in slightly different dialects.

Shadow AI is fragmentation's newest disguise: when staff bypass sanctioned tools, the organisation loses a reliable map of what data went where, and which controls (if any) still apply.

How do we address these issues? The key is connection: linking risks to controls, controls to assets, tests to evidence, and evidence to owners so that one update travels everywhere it needs to.

Why connection matters now

It matters because the perimeter is no longer yours. Verizon's 2025 DBIR says third-party involvement in breaches has doubled to 30%.[33] When a supplier incident lands, leaders don't ask how many tools you own. They ask what is affected, who owns it, and what proof you have, right now.

In that moment, 'connection' stops being an architecture preference and becomes a speed advantage: the ability to move from incident alert to credible impact statement without weeks of manual reconciliation.

[30] Tech Republic, TechRepublic.

[31] Cyber Magazine, Cyber Magazine.

[32] Tenable report, Tenable.

[33] Verizon report, Verizon.

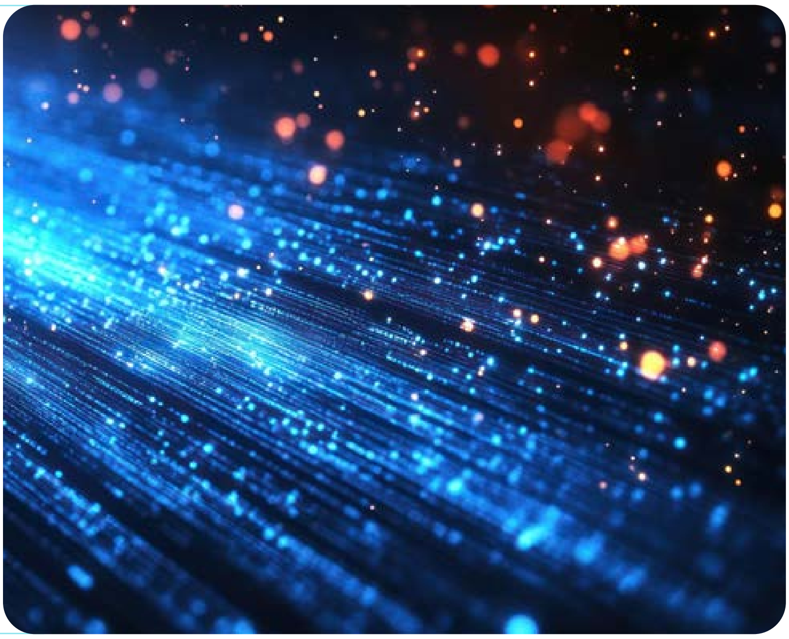
Reality check: MOVEit revisited

As noted earlier, attackers in 2023 exploited a flaw in MOVEit Transfer.

MOVEit mattered not just because it spread quickly, but because it exposed how few organisations could answer basic assurance questions at speed:

1. Where do we use this dependency? (asset and application linkage).
2. Which controls cover it and who owns them? (mapped controls with named accountability).
3. What evidence can we produce right now? (tests, results, and exceptions in one place).

The organisations that moved fastest weren't those with the biggest stack. They were the ones that could join the dots.[34]



IBM's 2025 report found organisations that used security AI and automation extensively cut breach time by 80 days and had US$1.9m lower average breach cost.[35] This kind of connection allows you to answer the real questions quickly: what changed, what's covered, and what's still open?

[34] CISA advisory, CISA.gov.

[35] Cost of a Data Breach Report, IBM.

7 Shrink the third-party blast radius.

Third-party risk used to be a specialist concern: contracts, questionnaires, a yearly audit if you were lucky. Now it is how modern organisations operate. Your perimeter is no longer a wall. It is a web of dependencies, such as cloud platforms, managed services, SaaS vendors, outsourced support, and a growing share of your attack surface sits outside your direct control.

That creates three uncomfortable truths.

First, exposure is shared. A weakness in a supplier can become your incident fast, because the same email threads, files and admin tools flow across organisational boundaries.

Second, responsibility is shared, whether you like it or not: customers and regulators will still hold you accountable for the impact.

Third, evidence pressure is shared. When something lands, leaders do not ask how many tools you own. They ask what is affected, who owns it, and what proof you can produce *now*.

Third-party reality check:

ENISA's 2025 threat landscape collected and analysed 4,875 incidents from open sources and member-state inputs:[36]

- Public administration is the most targeted sector in its dataset (38.2%).
- Phishing accounts for ~60% of observed initial access cases.
- Vulnerability exploitation represents 21.3% of initial access, rewarding speed.

The practical implication is not 'treat every supplier like a breach waiting to happen'. It is the opposite: be proportional.

Start with the suppliers that can cause the most harm: those tied to critical services, privileged access, sensitive data, or operational continuity. Then make three things unmissable: where they connect to your assets and services, who internally owns the relationship and the controls, and what evidence you can produce on demand.

Case example: Supplier identity compromise

In June 2025, New Zealand's National Cyber Security Centre described a near-miss in the energy sector: a "malicious email…originated from a compromised account owned by an external vendor", linking to a malware-embedded PDF hosted in the vendor's SharePoint. The energy company avoided impact because policies blocked the link and user sessions were revoked quickly, then the vendor confirmed the compromise.[37]

The lesson:

The lesson is blunt: supplier identity becomes customer impact unless you can shrink the blast radius through clarity, ownership and ready evidence, not bigger binders.

[36] Threat Landscape 2025, ENISA.

[37] Cyber Threat Report, NZSC.

8 Always-on readiness.

Readiness used to mean plans. Now it means tempo.

In addition to the now-familiar US$4.44m cost figure, IBM's Cost of a Data Breach Report reminds us that costs go up by the day. The uncomfortable detail is the clock: the same report shows a global breach lifecycle of 241 days.[38] That is not a security problem. It is an organisational coordination problem.

Meanwhile, the window between 'known' and 'too late' keeps collapsing. VulnCheck, tracking exploitation evidence in 1H 2025, found 32.1% of exploited vulnerabilities had evidence "on or before the day of the CVE disclosure", often meaning zero-days in practice.[39]

And in many regulated sectors, you're not only racing attackers, but also disclosure rules. Together, it's a stress test of whether your organisation can assemble a coherent, provable account of what happened.

As AI adoption accelerates, governance becomes part of readiness: Gartner warns that weak information governance can lead to unintended model inputs and downstream failures, from bad decisions to forced rollbacks.[40]

This is where manual effort quietly fails. Spreadsheets and point tools can store *facts*. They struggle to produce answers: what's affected, who owns it, what control covers it, and what evidence proves it, fast enough to brief executives, auditors and regulators without guesswork.

'Always-on readiness' is the opposite of maturity theatre. It's practical outcomes:

Faster detection because signals aren't trapped in silos

Defensible reporting because claims can be backed with evidence, quickly

Less scramble because ownership and mappings are already in place

Even IBM's numbers hint at the prize: organisations that extensively used security AI and automation averaged US$3.62m per breach versus US$5.52m for those that didn't: a reported US$1.9m gap.

This doesn't mean that AI is a universal positive for every enterprise. When used carefully and in a controlled fashion, it can detect breaches. When used without proper controls, it can increase exposure and risk.

Case example: Block agentic AI browsers – at least for now

What they are: Agentic browsers (AI browsers) can autonomously navigate the web and carry out tasks inside authenticated sessions.

According to Gartner, "CISOs must block all AI browsers in the foreseeable future" to minimise exposure.[41]

AI browsers can bypass traditional controls and create new risks, including sensitive data leakage, erroneous agentic transactions, and abuse of credentials.

The lesson:

Default settings often prioritise convenience over security, and may send active web content, browsing history and open tabs to a cloud-based AI back end unless hardened and centrally managed.

The lesson to learn here is not 'patch faster' – we all know that. It's that shrinking windows turn patching into a readiness discipline: you need measurable exposure visibility, clear ownership, and proof you can act before the call comes in.

[38] Cost of a Data Breach Report, IBM.
[39] State of Exploitation, VulnCheck.
[40] 2025 Q3 Emerging Risks, Gartner.
[41] Cyber research note, Gartner.

9 Self-test: how fragmented are your controls?

By now, the pattern should feel familiar. Modern cyber risk management isn't short of tools, frameworks or policies. It's short of joined-up proof.

You've seen how easily cyber turns into a coordination problem: too many dashboards, too many owners, too many versions of the same control, and then an incident arrives and demands one coherent answer.

You've also seen why fragmentation slows the response that matters most: the one that aligns technical action with executive decisions, regulatory obligations and clear communication.

So rather than introduce another survey, here's the only test that really counts.

Quick diagnostic: Three "can you answer this now?" checks

1. **Visibility: What's affected?** If a critical vulnerability drops at 4pm on a Friday, can you answer, without a scramble, where the dependency exists (apps, systems, suppliers) and what data it touches?
2. **Accountability: Who owns the control?** For the controls that matter most, is ownership named, current, and understood across teams, or does it live in people's heads (and holiday calendars)?
3. **Evidence: What proof do you have?** Could you produce evidence of control operation today (tests, results, exceptions, remediation) without stitching it together from spreadsheets, screenshots, and inbox archaeology?

A simpler set of 'fragmentation tells':

You can describe your controls, but you can't prove their effectiveness quickly

Ownership is clear in workshops, but blurry in practice

Reporting depends on heroic effort: someone 'pulls it together' each time

Evidence lives in too many places to be board-ready at short notice

Reality check: Manchester revisited

As discussed earlier, in June 2023, the University of Manchester publicly confirmed unauthorised access and said data had likely been copied.[42]

For leaders, that kind of statement triggers the same three questions, fast:

- What's affected? (systems, data, services)
- Who owns the response? (decision rights, internal and third-party)
- What proof can we show now? (evidence of controls, scope, containment)

If answering those requires a spreadsheet hunt, you don't just have a cyber problem. You have a fragmentation problem.

If you hesitated on any of the checks above, you're in the right place. The rest of this guide is about joining the dots, so ownership, controls and evidence move together, at incident speed.

[42] University of Manchester, University of Manchester.

10 What comes next: the era of provable resilience.

By the end of 2025, the direction of travel is no longer in doubt. Operational resilience has stopped being a program and started becoming a test.

Europe's DORA and Australia's CPS 230 are already in force. The UK's operational-resilience transition has ended. In the US, disclosure and notification clocks are tightening the same screw from different angles. The labels differ but the logic is converging; you must be able to explain disruption, quickly, with evidence.

That changes what 'good' looks like.

It is no longer enough to say you have controls. You need to show, at speed, that they are operating and what happens when they don't. Supervision is shifting from *'have you got a framework?' to 'prove your outcomes'.*

DORA pushes that mindset into ICT risk, testing and third-party oversight.[43] The UK regime focuses on staying within impact tolerances for important business services.[44] APRA is hardening expectations around operational risk and service providers.[45] And US rules increasingly reward organisations that can assemble a defensible narrative before rumours do.[46]

Then there is AI governance, to ensure you are dealing effectively with policies, shadow AI and emerging AI vectors such as browsers.

What should organisations do next?

Not 'buy more'. Do four practical things:

1. **Define what must not fail:** critical services and tolerances

2. **Map dependencies like you mean it:** including suppliers and privileged access

3. **Make ownership and evidence inseparable:** one control, one owner, one proof trail

4. **Rehearse the reporting clock:** so early warnings and executive updates are muscle memory, not improvisation

This should be your cyber end state: fewer surprises, faster answers, and a resilience story you can defend on the day you need it.

[43] EU DORA, EIOPA.

[44] Operational Resilience, FCA.

[45] CPS 230, APRA.

[46] Computer Security Incident Notification Requirements, Federal Register.

11 Next steps for your organisation

If this guide has highlighted one gap, it's not the absence of controls, it's the lack of joined-up proof.

The next step is to see what an **integrated cyber risk operating model** looks like in practice: where risks, controls, frameworks, evidence, assets, incidents and third parties are connected in one environment so you can answer "what's affected, who owns it, and what proof do we have?" at incident speed.

Choose the next step that fits where you are:

1. Explore the solution overview

Review our cyber solution for a clear view of how Protecht delivers clarity, speed and unified control through the cyber workspace, mapped frameworks, and continuous assurance.

Find out more

2. Book a short cyber workspace walkthrough

Schedule a 20-minute walkthrough focused on your reality (framework overlap, evidence capture, third-party blast radius, reporting pressure) to see how an integrated model reduces duplication and improves proof-readiness.

Request a demo

3. If you're actively improving assurance this quarter

Have a quick call to map where evidence breaks down across frameworks and teams, and what "one control, one owner, one proof trail" would look like in your environment.

Contact us

About the author.

Michael Franklin

Cyber Security Lead

Michael Franklin is Protecht's global Cyber Security Lead, with more than two decades of experience across cyber security, technology risk, and controls assurance in highly regulated environments.

He has held senior roles at Commonwealth Bank of Australia, Macquarie Group, and major universities including UNSW and the University of Sydney, where he has been directly accountable for translating cyber and technology risk into clear, defensible assurance for executives, boards, and regulators.

With a background that spans IT operations, audit, and enterprise risk, Michel has a practical view of where cyber programs break down during incidents and audits. He holds an MSc in Information Technology, a Graduate Certificate in Cyber Security, and industry certifications including CISM, CISA, and CDPSE.

ABOUT PROTECHT

Redefining the way the world thinks about risk.

While others fear risk, we embrace it. For over 25 years, Protecht has redefined the way people think about risk management. Through our people, we enable smarter risk taking by our customers to drive their resilience and sustainable success.

We help our customers increase performance and achieve strategic objectives through better understanding, monitoring and management of risk. We provide a complete solution of AI-enabled governance, compliance and risk management software supported by training and advisory services to businesses, regulators and governments across the world.

With our flagship SaaS GRC platform you can dynamically manage all your risks in a single place: enterprise risk, cyber and IT risk, incidents, vendor risk, operational resilience, business continuity, compliance, internal audit, workplace safety, and more.

We're with you for your full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com