CYBER ALCHEMY®
ASSESS·PROTECT·ENABLE

The Essential Guide to Cyber Threats in 2025

CYBERALCHEMY.CO.UK

Contents

Foreword

Every ambitious business is built on value – and in 2025, protecting and growing that value means being digitally resilient.

Neil Richardson
Founder
Cyber Alchemy

Today, when digital technology powers every aspect of operations, security isn't just a technical function – it's a foundation for trust, continuity, and competitive advantage.

You're probably aware of the cyber threats The most successful organisations are treating cybersecurity as a key strategic enabler - one that safeguards reputation, ensures operational stability, and underpins long-term business growth.

That's why we've written this guide.

This isn't fear-mongering or buzzwords. It's a straight-talking, insight-rich resource for leaders who want to protect their organisation's most valuable assets – and who understand that security, done right, is a growth lever.

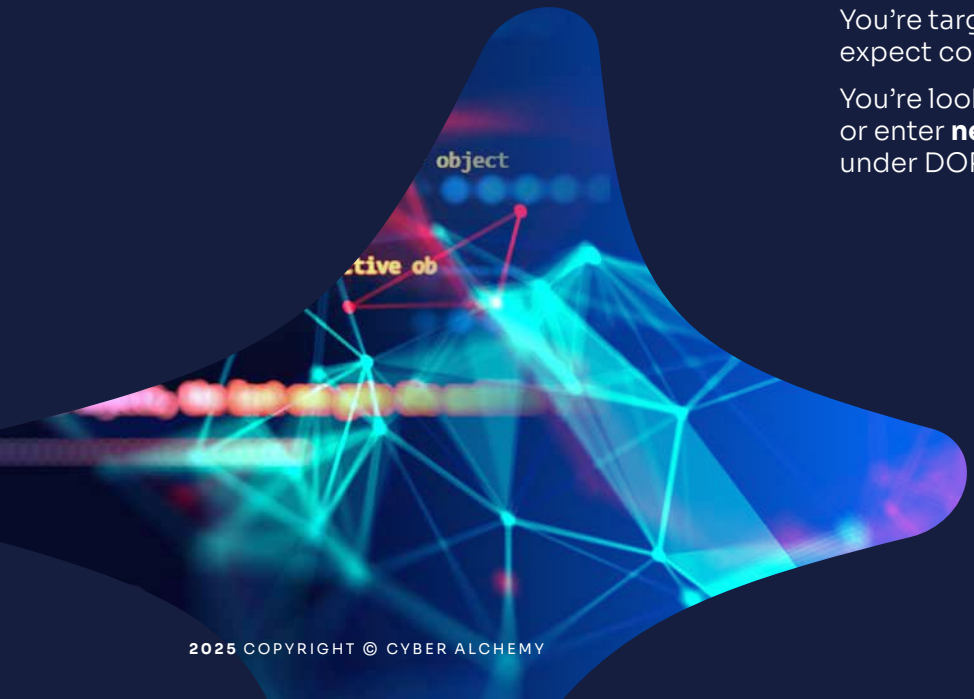
Inside, we'll help you:

- Understand the **real cost** of a breach in today's market
- Learn how cyber risk impacts shareholder value and business continuity
- Get clear on **emerging threats**, including deepfakes, AI attacks, and supply chain breaches
- Explore practical steps to build a modern, resilient, business-aligned security strategy

Use this guide however suits you: as a sanity check, a strategic conversation starter, or a roadmap to build from. Whether you're a founder, CFO, CTO or board member – if protecting value matters to you, this guide will too.

The role of cybersecurity compliance

We understand that you have lots of business priorities. Where should cybersecurity compliance be in this priority list?



Compliance should be seen as a strategic enabler, not just a box-ticking cost.

So, it should sit **near the top of your priority list**, especially if:

You're operating in **regulated markets** (like finance, healthcare, or critical infrastructure).

You're targeting **institutional clients** who expect compliance as table stakes.

You're looking to **scale**, secure **funding**, or enter **new jurisdictions** (like the EU under DORA).

Why it needs priority:

1) Regulatory risk = Business risk

Non-compliance = fines, restrictions, and reputational damage.

With DORA, NIS2, and others coming online, compliance failures may block growth.

2) Trust drives revenue

Compliance (when done well) reassures clients, partners, and investors.

It can help close deals faster–especially in sectors like FinTech or MedTech.

3) Good compliance makes you resilient

It overlaps with things you already want: strong cybersecurity, reliable systems, and business continuity.

That's a foundation for scale–not friction.

So where exactly should it sit?

Think of it like this:

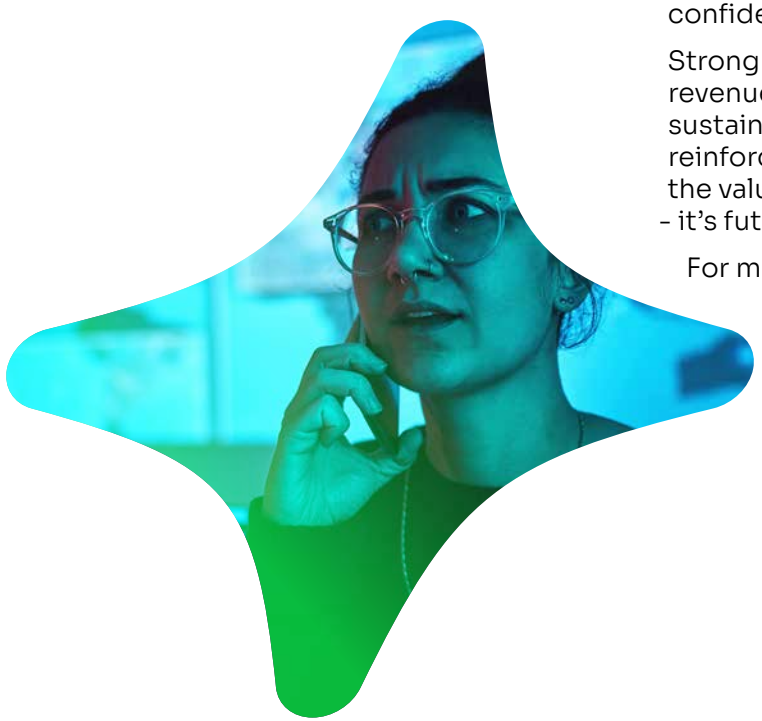
Priority Area	Role of Cybersecurity Compliance
Revenue growth	Opens doors to clients, reduces due diligence drag.
Operational efficiency	Prevents fines, avoids rework, reduces incident cost.
Innovation and technical development	Ensures new products meet regulatory requirements from day one.
Talent and culture	Builds a security – and ethics-aware workforce.
Funding / M&A	Makes due diligence smoother, increases valuation

If you're juggling a lot right now, you could treat cybersecurity compliance like a core layer under everything else:

"Build it into what you do– not as a side project, but as part of your business DNA."

The stakes

In 2025, cybersecurity is no longer just a technical issue – it's a value issue.



Every business is under pressure to grow, stay compliant, attract investors, and build customer trust. Cybersecurity plays a critical role in enabling that growth - by protecting what you've built and creating the confidence to scale.

Strong cyber resilience helps you preserve revenue, safeguard your brand equity, sustain operational momentum, and reinforce market credibility. It ensures that the value you're creating isn't just protected - it's future-proofed.

For most business leaders, the focus isn't just on avoiding cyber threats. It's about being confident that their business can respond, recover, and keep moving forward – no matter what. **See opposite and next page.**

Safeguard the trust that powers growth

Trust is one of your most valuable business assets – and great cybersecurity helps you preserve and strengthen it. Customers, partners, and investors are more likely to choose businesses that take data protection seriously.

66% of customers say they are more likely to engage with businesses they believe can protect their data.

Go beyond compliance – build confidence

Meeting regulatory standards is just the beginning. Businesses that demonstrate operational resilience signal strength, maturity, and leadership – gaining a competitive edge in an increasingly regulated world.

Tesco Bank was fined £16.4M for a breach that cost them just £2.26M in stolen funds.

Tesco Bank's case showed that regulators reward preparation and punish complacency. Proactive resilience is a strategic advantage.

Strengthen market perception

Cyber maturity isn't just about avoiding losses – it's a sign of capable leadership and sound governance. The market rewards businesses that treat digital risk like any other board-level responsibility.

Companies that lead on cybersecurity outperform over time, with stronger investor confidence and improved risk ratings.

BitSight & Solactive, 2022: Companies in the top cybersecurity tier delivered 1–7% annual outperformance, depending on sector.

Protect productivity and enable agility

Cyber resilience means fewer interruptions, smoother operations, and faster recovery when incidents do occur. It keeps your teams focused on delivering value, not responding to crises.

Businesses with robust response plans reduce downtime dramatically – protecting both revenue and reputation

Data from Accenture and World Economic Forum show mature firms bounce back quicker and win market trust.

Create the conditions for sustainable growth

Strong cybersecurity foundations open doors – especially in regulated sectors. They give customers, partners, and investors confidence – helping you win bids, secure funding, and scale without hesitation.

Organisations that demonstrate cyber maturity are more competitive in bids, more attractive to investors, and better positioned for long-term growth.

Lead with confidence

Cybersecurity is now a strategic function. Boards and executive teams that engage early and plan proactively are best placed to lead their organisations through uncertainty and change.

Only 14% of organisations feel confident they have the skills to manage cyber risk. Investing in capability is no longer optional – it's essential.

The World Economic Forum – Global Cybersecurity Outlook 2025 reports.

Cybersecurity done right changes everything

When cybersecurity is a route to new customers and new markets. It unlocks new markets, accelerates compliance, and gives leadership peace of mind.

Compliance becomes a badge of credibility, not a blocker.

Innovation moves faster – securely.

The business is protected, confident, and future-ready.

In short: cybersecurity isn't just a cost of doing business. It's how you **protect the value** you've built – and how you keep building more.

A cybersecurity posture for 2025

As threats have evolved, so too has the opportunity to use cybersecurity as a way to protect what matters most: your data, your reputation, and your ability to serve customers without disruption.

Whether you're scaling a fintech startup or managing risk across a global enterprise, the fundamentals remain the same: strong cybersecurity enhances trust, protects operational continuity, and helps safeguard the long-term value of your business.

Modern cyberattacks are designed with business impact in mind. They target the systems and relationships that create value – and that's exactly where resilient organisations stand out. A proactive, well-aligned cybersecurity strategy doesn't just keep threats at bay – it preserves your capacity to grow, innovate, and serve with confidence.

Ransomware: resilience over ransom

Ransomware continues to challenge businesses, but the solution lies in strengthening your continuity and recovery capabilities. By investing in secure backups, rapid detection, and clear response plans, organisations can minimise disruption, protect client trust, and avoid costly downtime.

Third-party confidence builds competitive advantage

As ecosystems grow, so do dependencies – and third-party risk has become a key consideration for operational resilience. Companies that assess, monitor, and secure their supplier relationships not only reduce risk but also build stronger partnerships and supply chain confidence.

Human risk is now a business opportunity

AI-driven scams and deepfake attacks are a reminder of how important your people are to your resilience.Studies consistently show that human error is a factor in the majority of breaches, with some analyses attributing over 80% of successful attacks to human or behavioural gaps – making people a critical line of defence. Empowering staff with clear guidance, secure tools, and regular awareness training turns your workforce into a powerful defence – and builds a more security-aware culture.

Identity and Access: The Foundations of Trust

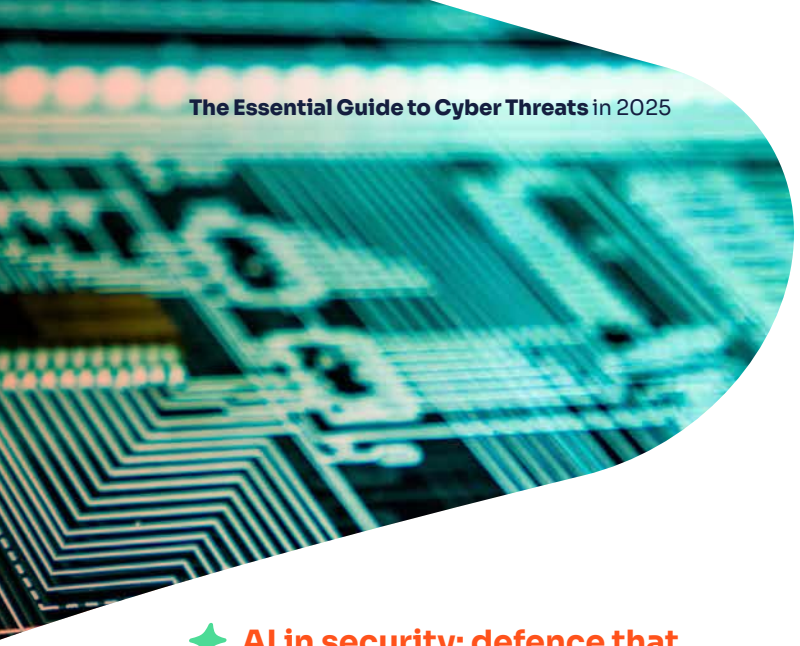
Strong identity and access management is more than a control – it's a cornerstone of digital trust. Protecting credentials, using multi-factor authentication, and reducing unnecessary access across the organisation are simple steps that preserve integrity and reduce risk at scale.

Remote and hybrid work: secure by design

Remote and hybrid work are here to stay. Building secure-by-default systems, wherever people work, ensures flexibility doesn't come at the cost of visibility or control. This is about empowering your teams to work safely, efficiently, and confidently from anywhere.

Cloud confidence through configuration

Cloud platforms offer agility and scalability – but only if they're well configured. Organisations that embed security into cloud adoption from the start benefit from faster innovation, fewer surprises, and greater peace of mind.



AI in security: defence that learns and adapts

AI isn't just being used by attackers – it's powering better, faster, and more adaptive defences. By leveraging smart detection, automated response, and predictive analytics, businesses can stay one step ahead and focus on opportunities, not just risks..

Geopolitics: cyber attacks linked to global tensions:

While global tensions have led to an increase in cyber activities linked to state actors, proactive businesses can turn preparedness into strategic advantage. Understanding that these attacks–such as espionage, ransomware, or data theft–can reach beyond governments to commercial sectors, gives your business clarity. For organisations operating internationally or in sensitive industries, enhancing visibility, preparedness, and resilience positions you ahead of the curve, empowering you to confidently navigate complex global landscapes.

Human risk and skills shortage

In 2025, cybersecurity success rests as much on your people as on technology. Yes, security teams face challenges–burnout, talent shortages, and limitations of traditional awareness training–but forward-thinking businesses can meet these challenges by prioritising human-centric risk management. Embrace engaging training methods like microlearning, gamified scenarios, personalised role-based simulations, and behavioural nudges. Investing in your people transforms human risks into human strengths, creating a resilient, skilled, and motivated workforce ready to tackle future threats.

Navigating an interconnected business world with confidence

In a world of increasing complexity and interdependence, resilient businesses take a strategic approach to cybersecurity. They align it with business goals, regulatory requirements, and customer expectations – not as a reactive function, but as a foundation for growth.

Building resilience and awareness

At Cyber Alchemy, we help businesses protect and grow what they've built.

Because real resilience isn't just about stopping attacks – it's about enabling your business to move forward with clarity, confidence, and control.

That's why a cybersecurity strategy in 2025 can't rely on static tools or old frameworks. **It needs to be proactive, dynamic, and aligned to your business goals.**

This guide will show you how.

The problem with 'major incidents'

When a cyber attack hits the headlines, it's usually because it's big – a major corporation, a household name, a jaw-dropping figure like **"$30 million in losses."** But this kind of coverage, (while attention-grabbing) doesn't always paint a useful picture for the average business.

In reality, most cyber incidents don't make the news. They're quieter, messier, and more common. And while the impact can still be severe, the response doesn't need to be panicked or overblown.

A sensible cybersecurity posture is measured, non-hysterical, and shaped by your business context. You don't need to live in fear, but you do need to be informed. Know the risks, understand the likely impact, and take practical steps to protect yourself.

By the end of this guide, you'll have a clear, straightforward way to build a cybersecurity strategy that's right for your business.

What happens when you have a robust security posture?

A strong security posture isn't about eliminating all risk – that's impossible and financially un-feasible. It's about being prepared, responsive, and resilient when things do go wrong. When your cybersecurity strategy is aligned to your business context, the benefits go far beyond just 'not getting hacked.'

Here's what a well-prepared business looks like in practice:

1) Business as usual – even when threats arise

Incidents may still happen, but they don't grind everything to a halt.

Your teams know the drill. Response plans are in place. Customers stay informed, services keep running, and you stay in control.

The difference isn't whether a threat appears – it's how quickly and effectively you bounce back.

2) Customer and partner confidence

When clients ask about your security policies (and they will), you've got clear answers.

A strong security posture builds trust – and for many organisations, it's the difference between winning or losing a major deal.

Cyber resilience has become a business asset, not just a compliance requirement.

3) Less downtime, more productivity

With the right tools and processes in place, you reduce the risk of long outages.

And if something does go wrong, you've already rehearsed the playbook.

That means less scrambling, less firefighting, and more time focused on what matters – your customers and your growth.

4) Stronger internal culture

Good security isn't just technical – it's cultural.

When people know how to spot threats, when policies are clear (and actually followed), you reduce the risk at every level.

Your team becomes part of the solution, not a weak point in the chain.

5) Board-Level confidence

Boards and investors are increasingly focused on cyber readiness.

When they see that security is embedded into your operations – not just tacked on – it inspires confidence and reduces anxiety.

You're not just protecting the business; you're protecting its future.

6) Growth accelerator

Whether you're scaling, fundraising, or preparing for a new market, security is no longer a blocker – it's a foundation.

A mature security posture clears the path for growth by keeping risks in check and reducing the chance of last-minute surprises.

The bottom line?

Robust cybersecurity is good business. It gives you the space to grow, the confidence to act, and the resilience to handle whatever comes next.

Where does cybersecurity add value?

For modern businesses, the real opportunity lies in what security makes possible. When done right, cybersecurity doesn't just protect the value you've built – it actively helps you unlock more.

Move fast, without inadvertently introducing risk

Startups and scaleups need to move fast. They're innovating, shipping, growing – and burning cash. Security, when done badly, slows everything down. But when it's built into the business strategy, it becomes a launchpad. Cybersecurity enables teams to adopt new technologies like AI and cloud infrastructure without unknowingly introducing risk. You get speed and confidence – a combination that's essential for businesses looking to lead.

Access more markets with fewer barriers

Procurement teams are getting stricter. Regulatory frameworks are getting tighter. And large customers increasingly ask detailed questions about your security posture before they'll even sign a contract. With strong cybersecurity in place – and certifications like ISO 27001 or Cyber Essentials – you can move through due diligence faster and avoid being caught out by unexpected security demands. Cyber becomes a passport, not a roadblock.

Be ready for funding, exits, and growth

Whether you're raising a new round, preparing for acquisition, or entering a regulated sector – security matters. Investors and acquirers now see cybersecurity as a proxy for operational discipline. A mature approach, documented processes, and resilience planning show that your house is in order – which can be the difference between moving forward and stalling out in due diligence.

Meet regulatory and compliance requirements

From DORA to GDPR, the regulatory environment is only getting more complex. Having a security strategy that aligns with these frameworks means you avoid last-minute scrambles, rushed fixes, and unnecessary fines. When cybersecurity is embedded from the start, you meet requirements with ease – and often well before you're asked.

Build trust with clients and partners

Trust is currency. When clients know their data is safe with you, they stay longer, spend more, and refer others. The same goes for partners and suppliers – many of whom now conduct security audits as standard. A business that takes cybersecurity seriously becomes a safer bet – and in some industries, the only viable choice.

Stay resilient when things go wrong

No system is perfect. Even the best defences can be breached. But what happens next matters just as much. Businesses with a solid response plan bounce back faster, minimise disruption, and protect their reputation. Resilience is the true mark of a mature security posture – and it's what allows you to operate confidently, even in a crisis.

Be ready for funding, exits, and growth

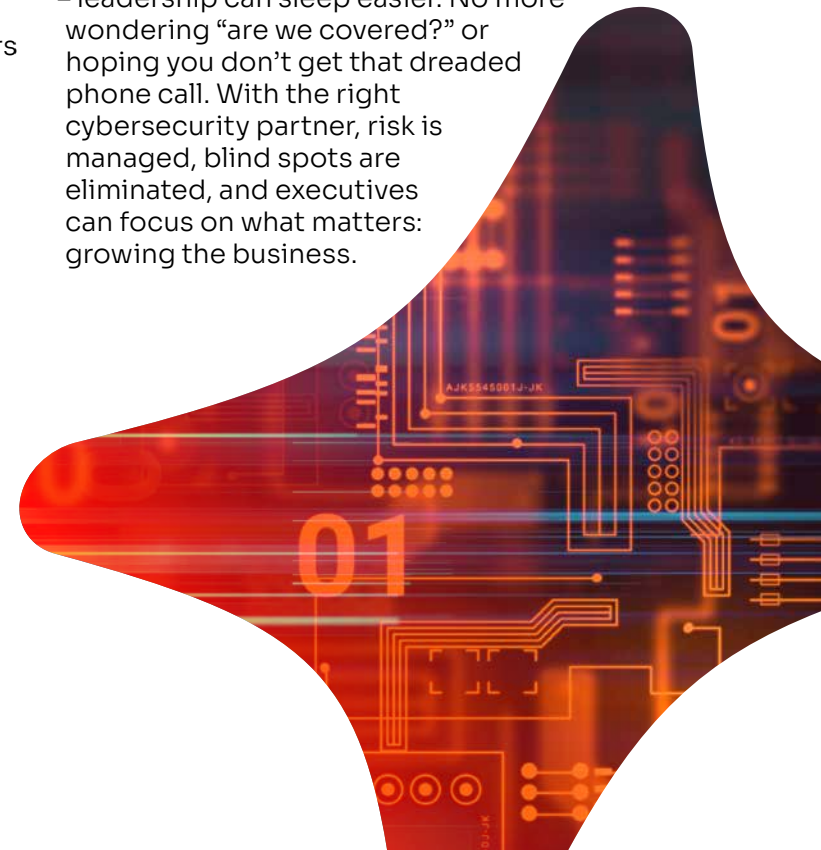
Whether you're raising a new round, preparing for acquisition, or entering a regulated sector – security matters. Investors and acquirers now see cybersecurity as a proxy for operational discipline. A mature approach, documented processes, and resilience planning show that your house is in order – which can be the difference between moving forward and stalling out in due diligence.

Meet regulatory and compliance requirements

From DORA to GDPR, the regulatory environment is only getting more complex. Having a security strategy that aligns with these frameworks means you avoid last-minute scrambles, rushed fixes, and unnecessary fines. When cybersecurity is embedded from the start, you meet requirements with ease – and often well before you're asked.

Peace of mind

When cybersecurity is treated as a strategic function – not just an IT checkbox – leadership can sleep easier. No more wondering "are we covered?" or hoping you don't get that dreaded phone call. With the right cybersecurity partner, risk is managed, blind spots are eliminated, and executives can focus on what matters: growing the business.



What threats (and defences) are on the horizon?

The cyber threat landscape isn't just growing – it's evolving.

While many of the threats we face today are familiar (ransomware, phishing, misconfigured systems), the tools and tactics used to execute them are changing fast. Technologies that enable business growth – like AI, cloud, and remote collaboration – are also being used by malicious actors to scale their attacks and exploit new vulnerabilities.

This section outlines several fast-evolving technologies and how they are shaping both the **risks** and **defences** that leaders need to be aware of in 2025 and beyond.

Machine learning and artificial intelligence (AI)

AI is one of the most disruptive forces in cybersecurity – for defenders and attackers alike. On one hand, AI offers huge advantages in detecting and responding to threats at scale. On the other, the same tools can be used to create more targeted, adaptive, and hard-to-detect attacks. In 2025, the line between human and machine-generated cybercrime has blurred – and that creates new challenges for business leaders.

The threats

Adversarial attacks

Cybercriminals are learning how to manipulate AI systems directly feeding them deliberately crafted inputs that cause misclassification or suppression of legitimate threats. These "adversarial" attacks could result in AI systems ignoring malware, misinterpreting behaviour, or even blocking legitimate users.

AI-powered social engineering

We're seeing a rise in AI-generated phishing content that mimics real employees or executives not just in writing, but in voice and video. Tools like FraudGPT and WormGPT can create convincing messages at scale, dramatically increasing the success rate of scams.

Data exposure and privacy risks

As organisations increasingly adopt AI, particularly generative models, it's critical to establish clear governance for secure and ethical deployment. This includes implementing robust internal policies that prevent staff from inputting confidential or sensitive data into public AI tools, and proactively testing AI models for security, privacy, and compliance vulnerabilities. Prompt injection, training data exposure, and manipulation of model outputs are emerging threats. With regulations like the EU AI Act on the horizon, periodic audits and documented AI governance practices are becoming essential, not optional.

Over-reliance on automation

As AI systems take on more responsibility in security operations, some businesses risk becoming too dependent on them – assuming their systems are "safe" without human oversight. When AI fails, or is faced with a novel threat it doesn't recognise, the result can be a dangerous blind spot.

Weaponisation by attackers

Just as AI can be used to defend, it can also be weaponised. Criminal groups are already using AI to automate vulnerability scanning, generate exploit code, and adapt malware behaviour in real time. These tools lower the barrier to entry for less-skilled attackers – while scaling up the reach of more advanced ones.

Deepfakes and executive impersonation

Attackers are leveraging deepfake technology for executive impersonation — via video, voice, or synthetic media. These tactics can bypass human verification and even defeat voice-based multi-factor authentication (MFA), increasing the risk of high-impact fraud and data breaches.

The defences

Adaptive threat detection

AI-enabled defence platforms are now capable of analysing massive volumes of traffic, behaviour, and device telemetry in real time – spotting subtle patterns that traditional tools miss. These systems constantly learn and refine themselves, making them ideal for identifying emerging threats.

Security automation

Routine security tasks – from patch management to access monitoring – are increasingly being handled by AI-driven systems. This reduces human error, accelerates response times, and allows human teams to focus on high-risk or complex threats.

Predictive analytics

By ingesting global threat intelligence and combining it with internal activity data, AI tools can predict future attack paths and identify which assets or users are likely to be targeted. This "anticipate and pre-empt" model is rapidly replacing the old "detect and respond" approach.

Human-AI collaboration

The best results come when humans and machines work together. In leading organisations, AI augments decision-making – helping analysts prioritise risks, understand context, and respond faster. AI can also assist with real-time decision support during phishing attempts or social engineering calls, flagging unusual requests and prompting human verification.

Overall

Like most transformative technologies, AI is a double-edged sword. It offers enormous potential for improving security – but it also empowers attackers with speed, scale, and deception tactics that were previously unimaginable.

The organisations that thrive in this environment are the ones who **embrace AI defensively** while **remaining vigilant about its risks**. The pace of change is rapid – but with the right approach, AI can be a force multiplier for cyber resilience.

Remote and hybrid work

Remote and hybrid working have become the norm – not the exception.

While this shift has brought flexibility and improved productivity for many organisations, it has also reshaped the cyber threat landscape.

The lines between corporate and personal devices, networks, and behaviours have blurred. What used to be secured behind office firewalls is now being accessed from coffee shops, living rooms, and mobile phones. This decentralisation has created a broader attack surface – and one that's far more difficult to monitor or control with traditional methods.

The threats

Ransomware

Ransomware tactics continue to evolve. Beyond simple data encryption, attackers increasingly focus on business disruption and multi-extortion exfiltrating data, targeting customers or partners, and leaking information to maximise pressure. Resilience strategies must therefore go beyond backup, prioritising business continuity, comms planning, and legal readiness.

Expanded attack surface

With employees working across multiple devices and locations, businesses face a wider array of entry points for attackers. Unsecured home Wi-Fi, shared devices, or outdated personal laptops can all become weak links in an otherwise secure environment.

Phishing and social engineering

Remote workers are often isolated from the usual safety nets – no colleague nearby to double-check a suspicious email, no IT team walking the floor. Attackers exploit this with well-timed phishing campaigns and urgent-sounding requests that trick employees into clicking links or transferring funds.

Shadow IT and unauthorised tools

In a remote-first world, employees often adopt their own tools to "get the job done" – whether it's sharing files via personal Dropbox accounts or messaging clients through WhatsApp. This creates blind spots for security teams and increases the risk of data leakage.

Device sprawl and endpoint risk

When every employee has multiple devices – laptop, mobile, tablet – and uses them interchangeably for work, endpoint management becomes complex. Lost devices, lack of updates, and poor password hygiene create real risks for data exposure or compromise.

VPN fatigue and misuse

Many organisations rely on virtual private networks (VPNs) to secure remote access – but poor configuration, expired certificates, or reliance on shared credentials make them a frequent target. Attackers often exploit unpatched VPN gateways to gain access to internal systems.

The defences

Endpoint detection and response (EDR)

EDR tools allow businesses to monitor activity on remote devices in real time – detecting unusual behaviour, isolating compromised machines, and rolling back changes from ransomware or malware. This provides a crucial layer of visibility and control outside the office.

Strong identity and access management (IAM)

With users logging in from everywhere, verifying who they are becomes critical. Multi-factor authentication (MFA), single sign-on (SSO), and conditional access policies help ensure that only the right people get access – from approved devices and locations.

Secure collaboration platforms

Replacing ad hoc tools with company-approved, secure platforms (e.g. Microsoft Teams, Google Workspace, Slack with DLP policies) ensures that conversations and data stay within protected environments – while still enabling agile teamwork.

User awareness and training

Phishing simulations, policy refreshers, and bite-sized cybersecurity training help keep remote teams alert. Just because someone's working from home doesn't mean they should be out of the security loop. Awareness needs to be continual, contextual, and engaging.

Zero trust networking

Zero Trust assumes that every device, user, and connection is untrusted by default. This approach is ideal for remote work environments – where internal and external traffic blends, and network boundaries are no longer clear.

Overall

Remote and hybrid work are here to stay – and so are the risks they introduce.

But with the right mix of technology, training, and mindset, businesses can protect productivity and security. The key is visibility, context, and control – without getting in the way of how people actually work.

When cybersecurity adapts to the way your team operates – instead of forcing the reverse – everyone wins.

Cloud (mis)configuration

Cloud platforms are now the foundation of most modern businesses. From file storage and databases to full-blown infrastructure, organisations rely on services like AWS, Azure, and Google Cloud to operate at scale. But while cloud has brought flexibility and efficiency, it has also introduced new and often invisible security risks – especially when services are poorly configured.

Misconfigurations remain one of the most common and preventable causes of cloud-related data breaches. And because cloud environments are constantly evolving, even secure setups can drift into vulnerability over time.

The threats

Publicly exposed data

One of the most frequent issues is cloud storage buckets (e.g., S3) being left open to the public internet – either by mistake or through misunderstood settings. This has led to high-profile leaks of sensitive information, including customer records, source code, and internal documents.

Overly permissive access

Access control in cloud environments can be complex, and mistakes are common. Admin privileges might be granted too broadly, service accounts may be misused, or users may retain access long after they've left the company – increasing the risk of compromise or insider threats.

Unpatched virtual machines and services

While cloud providers secure the infrastructure, businesses are responsible for what they run on it. Unpatched software, legacy systems, and insecure APIs running in virtual machines or containers create opportunities for attackers – especially when internet-facing.

Credential exposure in repos or logs

In fast-moving DevOps environments, it's not uncommon for cloud credentials or secrets to accidentally get committed to public code repositories, logs, or documentation – giving attackers an easy way in, often without being noticed until much later.

Shadow cloud services

Departments or teams might spin up their own cloud services outside the central IT governance process. These "shadow" environments often go unmonitored and unpatched, leaving critical gaps in visibility and defence.

The defences

Cloud security posture management (cspm)

CSPM tools automatically scan cloud environments for misconfigurations, poor access controls, and other weaknesses. They provide continuous monitoring and remediation recommendations – helping security teams stay ahead of drift and reduce manual oversight.

Principle of least privilege

By limiting every user and service account to the bare minimum permissions needed, businesses can reduce the impact of credential compromise or accidental misuse. Regular reviews and automated access expiry help enforce this principle at scale.

Secrets management

Proper use of secrets vaults (e.g. HashiCorp Vault, AWS Secrets Manager) ensures that credentials, API keys, and sensitive config data are stored securely – not hardcoded in scripts or stored in plaintext files.

DevSecops integration

Embedding security into the development pipeline helps catch risks earlier. This includes scanning Infrastructure-as-Code (IaC) templates, enforcing policies before deployment, and enabling security teams to collaborate with developers without slowing them down.

Multi-cloud governance

As more businesses adopt multiple cloud providers, unified visibility becomes essential. Centralising policies, identity controls, and compliance monitoring across platforms helps reduce fragmentation and ensures a consistent security baseline.

Overall

Cloud infrastructure enables scale, agility, and innovation – but only if security keeps pace.

The challenge isn't just defending against outside attackers – it's **maintaining control in an environment that changes every day**.

Security leaders need to treat the cloud not as a single system, but as a living ecosystem. The right tools and governance ensure that your cloud grows safely – without creating unseen risk in the background.

Supply chain risk

You can have strong internal security – but still be vulnerable.

In 2025, attackers are increasingly targeting the trusted third parties that connect to your business: software vendors, IT service providers, cloud platforms, payroll processors, even law firms. This is the new supply chain risk – and it's becoming one of the most exploited weak points in business security today.

The issue? These relationships are built on trust – and that trust is now being weaponised.

The threats

Third-party software compromise

One compromised update – like in the infamous SolarWinds breach – can give attackers access to hundreds of downstream customers. This kind of attack is hard to detect, since it appears to come from a trusted source. It's a modern form of Trojan horse, at enterprise scale.

Service provider vulnerabilities

IT providers, MSPs, and even accounting firms often hold privileged access to internal systems. If their credentials or systems are breached, yours can be too – and you may not even realise it's happening until damage is done.

Open source dependencies

Most modern applications are built on open source libraries. These are often maintained by volunteers – and while they're widely used, they aren't always secure. Attackers can inject malicious code into popular packages, affecting thousands of companies at once.

Delayed disclosure

Even when a breach happens, you might not hear about it in time to respond. Many organisations delay disclosure to investigate, contain, or protect their reputation. That means your systems could be compromised by proxy, without your knowledge.

Compliance and regulatory fallout

If a supplier's breach exposes your data, you may still be held responsible – especially under GDPR, DORA, or industry-specific frameworks. And if due diligence processes weren't followed, legal liability can land squarely on your business.

The defences

Third-party risk management (TPRM)

Structured TPRM programs go beyond one-time supplier reviews. They include pre-engagement risk assessments, ongoing monitoring, and contract clauses that require cyber hygiene, certifications, and breach notification timelines.

Zero trust supply chain access

Vendors and partners should never have broad, unchecked access. Limit connections with the **principle of least privilege**, monitor usage patterns, and segment network access to reduce the blast radius of compromise.

Software bill of materials (SBOM)

An SBOM helps track every component in your tech stack – including open source libraries – so you can quickly identify exposure when a vulnerability is disclosed. This is becoming a key requirement in regulated environments.

Vulnerability disclosure and patch SLAs

Work with suppliers to ensure they have clear processes for reporting vulnerabilities – and holding them to defined patch timelines. Include this in your contracts, especially for mission-critical services or software.

Cyber insurance with supply chain clauses

Ensure your cyber policy explicitly covers supply chain-related incidents, including losses from third-party downtime or breach liability. Many insurers now require proof of third-party risk governance to provide coverage.

Overall

Your business doesn't exist in a vacuum – it runs on a network of dependencies.

Every supplier, tool, and platform you use introduces some level of cyber risk – whether you see it or not.

In 2025, smart organisations treat supply chain security as a **core function** – not a compliance formality. Because in a hyper-connected world, your risk is **shared risk** – and you're only as secure as your weakest trusted connection.

Credential theft and identity risks

In many cyber attacks, the attacker doesn't need to "break in" – they just log in.

Stolen usernames and passwords are one of the most common entry points for breaches. In 2025, identity has become the new perimeter – and attackers know it. They're constantly harvesting, guessing, buying, and tricking their way into accounts.

Once inside, they can move laterally across systems, escalate privileges, and often remain undetected for weeks. Whether it starts with a compromised email, a leaked credential from a third-party breach, or a clever phishing attempt – identity-based attacks are now at the heart of modern cybercrime.

The threats

Credential stuffing

Attackers use credentials leaked in previous breaches and try them across multiple platforms – banking on the fact that users often reuse the same passwords across accounts. Automated tools make it easy to test millions of combinations in minutes.

Phishing and MFA fatigue

Phishing is getting more sophisticated – with AI-generated messages, urgent tone, and perfect branding. Even when MFA is in place, attackers exploit "push bombing," bombarding users with approval requests until they accept out of confusion or fatigue.

Session hijacking and token theft

With so many systems relying on cloud logins and browser sessions, attackers are now targeting session tokens stored in browsers or memory. Once stolen, these can grant access even without a password or MFA.

Insider threats and privilege abuse

Not all credential-based attacks come from the outside. Disgruntled employees, over-provisioned contractors, or even well-meaning staff with too much access can cause just as much damage. Over time, privileges expand – but they're rarely reviewed or revoked.

Password sharing and poor hygiene

In fast-paced environments, staff often share logins, reuse weak passwords, or store them insecurely (in spreadsheets, emails, or browser autofill). These bad habits create easy opportunities for attackers.

The defences

Strong identity and access management (IAM)

IAM systems allow businesses to tightly control who has access to what – and when. This includes enforcing complex passwords, integrating single sign-on (SSO), enabling MFA across all systems, and logging all access activity for review.

Least privilege and just-in-time access

Staff and service accounts should only have access to what they need – and only when they need it. Just-in-time access reduces standing permissions, while privilege reviews and expiry policies help prevent accumulation of unused high-level access.

Password managers and secrets vaults

Company-wide use of password managers ensures employees aren't reusing or poorly storing credentials. For systems and APIs, secrets vaults (e.g., AWS Secrets Manager, HashiCorp Vault) provide secure, auditable storage for critical authentication data.

Phishing-resistant MFA

Modern MFA tools – like FIDO2 security keys, biometrics, or authenticator apps with number matching – are significantly harder to trick than SMS codes or push notifications. These newer methods help neutralise phishing and MFA fatigue attacks.

User awareness and culture change

Building a culture of identity hygiene – where people think twice before clicking links or approving login prompts – is key. Training, simulated phishing tests, and open reporting channels encourage vigilance and empower employees to spot threats early.

Overall

Identity is the front door to your organisation – and attackers are learning how to pick the lock.

A modern cybersecurity strategy must treat identity not just as a technical function, but as a core business risk. The good news? With the right policies, tools, and culture, credential-based attacks are among the **most preventable** threats you face.

But they require constant attention – because credentials are everywhere, and attackers only need one.

Quantum and future threats

Some cyber threats are immediate. Others are building in the background – slow, technical, and easy to ignore... until they aren't.

Quantum computing falls squarely into the latter category. While we're still years away from practical, large-scale quantum systems that can break today's encryption, the risk is already taking shape. State-backed actors and sophisticated cybercriminals are believed to be collecting encrypted data now with the intent to "steal now, decrypt later" – waiting for quantum tools to catch up.

For businesses that handle long-lived sensitive data – think legal, healthcare, financial, or government-linked organisations – that's a risk that can't be ignored. But quantum isn't the only "future" risk. Advancements in autonomous malware, offensive AI, and novel infrastructure (like edge computing and decentralised cloud) are all reshaping the landscape.

The threats

Post-quantum cryptography risk

Most of today's encryption relies on algorithms that quantum computers will eventually be able to break – particularly RSA and ECC. When that happens, anything encrypted today without future-proofing could be instantly exposed.

"Harvest now, decrypt later" attacks

Advanced threat actors are already intercepting encrypted traffic and storing it for the long term. Once quantum decryption becomes viable, they'll be able to retroactively access years of sensitive communications or transactions.

Disruption of trust models

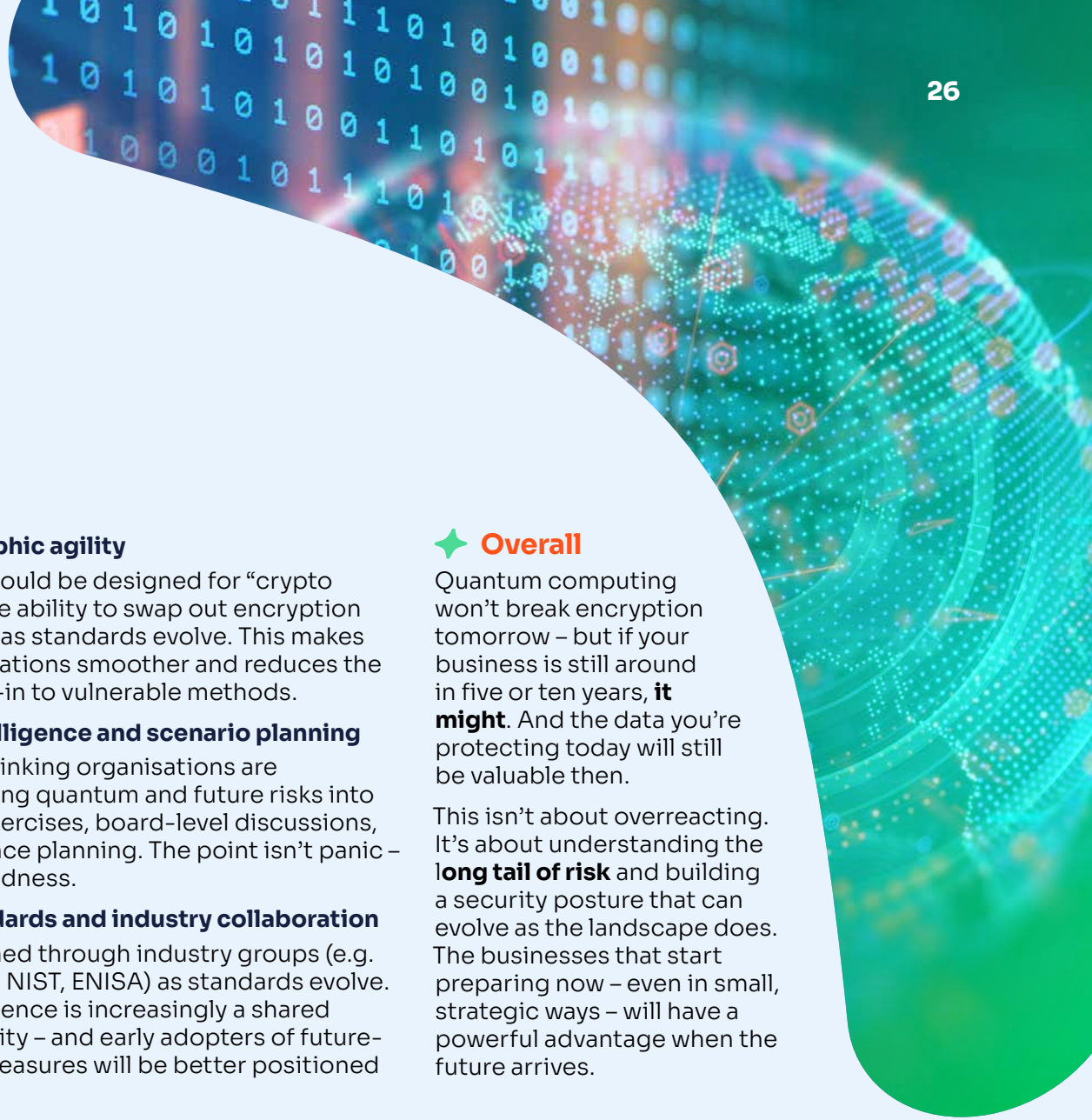
Quantum tech could undermine the digital certificates and trust infrastructure that underpins secure web traffic, digital signatures, and identity verification. If attackers can forge certificates, they can impersonate websites, emails, or even entire organisations.

Rise of autonomous offensive tools

Beyond quantum, the future threat landscape includes self-replicating AI malware, tools that adapt on the fly, and autonomous bots capable of lateral movement and privilege escalation – without human guidance. These tools are already being prototyped.

Increased attack surface via emerging tech

New infrastructure like IoT, edge computing, and containerised microservices introduce complexity – and with it, more potential for misconfigurations, API vulnerabilities, and data leakage, especially when security is an afterthought.



The defences

Begin migration to post-quantum cryptography

NIST has already published draft standards for post-quantum algorithms. Businesses that handle high-value or long-lived data should start evaluating and testing quantum-resistant encryption now – especially for VPNs, secure email, and archived backups.

Data classification and retention audits

Knowing what data needs long-term protection – and what doesn't – is key. Organisations should assess how long their sensitive data must remain secure, and reduce the risk by limiting unnecessary retention of high-value information.

Cryptographic agility

Systems should be designed for "crypto agility" – the ability to swap out encryption algorithms as standards evolve. This makes future migrations smoother and reduces the risk of lock-in to vulnerable methods.

Threat intelligence and scenario planning

Forward-thinking organisations are incorporating quantum and future risks into tabletop exercises, board-level discussions, and resilience planning. The point isn't panic – it's preparedness.

Track standards and industry collaboration

Stay informed through industry groups (e.g. NCSC, ISO, NIST, ENISA) as standards evolve. Cyber resilience is increasingly a shared responsibility – and early adopters of future-proofing measures will be better positioned to lead.

Overall

Quantum computing won't break encryption tomorrow – but if your business is still around in five or ten years, **it might**. And the data you're protecting today will still be valuable then.

This isn't about overreacting. It's about understanding the l**ong tail of risk** and building a security posture that can evolve as the landscape does. The businesses that start preparing now – even in small, strategic ways – will have a powerful advantage when the future arrives.

What to do next?

Understanding the risks is important – but it's only the beginning. The real value comes from knowing how to respond, with calm, clarity, and a plan that fits your business.You don't need to become a cybersecurity expert overnight. And you don't need to panic about closing every possible gap immediately. What you do need is a focused, practical approach – one that gives you confidence, not confusion.

Here's how to get started:

1) Understand your cyber risk profile

Start by identifying what matters most:

- What data is most sensitive?
- What systems are essential to your day-to-day operations?
- Where are you already strong – and where could you improve?

This isn't about overcomplicating things. It's about getting honest visibility into your current posture, so you can make smart, informed decisions.

It's also important to understand that not all threats are created equal. Some cyber risks are **predictable and measurable** – like known vulnerabilities or common attack methods. Others involve **uncertainty** – new threats, human error, or supply chain risks you can't always see coming.

At Cyber Alchemy, we use a three-phase approach to help businesses deal with both:

- **ASSESS:** Identify and measure your current exposure – what's at risk, what's urgent, and where to act.
- **PROTECT:** Fix the issues you can control and build strong, tested defences.
- **ENABLE:** Prepare for the unpredictable – building resilience, agility, and long-term confidence.

Understanding the difference between **risk** and **uncertainty** helps you stay focused and adaptable – no panic, just progress.

2) Connect security to business value

Cybersecurity isn't just an IT issue – it's a business enabler.

The right security strategy helps protect your reputation, ensure continuity, maintain customer trust, and support long-term growth. When your approach to cybersecurity is aligned with your business goals, it becomes a source of strength, not just a safeguard.

3) Focus on the fundamentals

The latest tech helps defend against advanced threats, but the basics still stop most attacks - and they're often the fastest wins:

- Strong password management and MFA
- Secure cloud setup
- Regular updates and patching
- Ongoing staff awareness
- A rehearsed incident response plan

With the right support, these foundations can be put in place quickly – and they deliver outsized value

4) Know what good looks like

There are clear, achievable standards that can guide your strategy: Cyber Essentials, ISO 27001, NIST, CIS - as well as industry-specific frameworks. You don't need to tick every box at once, but knowing where you're headed helps keep your efforts focused and meaningful.

5) Get the right support

You don't have to tackle this alone.

The cybersecurity landscape moves quickly, and it's not realistic to expect internal teams to handle everything on their own. That's where a trusted partner can make all the difference.

At Cyber Alchemy, we help fast-growing businesses build cybersecurity strategies that are smart, sustainable, and tailored to their goals. Whether you're starting from scratch, reviewing your current posture, or looking for a sounding board – we're here to help you move forward with clarity and confidence.

From insight to action: what you can do right now?

Quick wins and critical questions for leadership teams to steer immediate progress.

While some improvements take time, budget, and planning – others start with the right questions. The following actions and prompts are designed for leadership teams to use immediately. They don't require full transformation, but they do spark visibility, accountability, and next steps across your organisation.

1) Visibility and risk understanding

Why it matters: You can't secure what you can't see.

Questions to ask your team:

- Do we have a current inventory of our critical assets – systems, data, third parties?
- Have we mapped where our most sensitive or regulated data sits?
- Can we articulate our top 3 cybersecurity risks in business terms (e.g., financial loss, reputational damage)?

2) Access, authentication and identity

Why it matters: Most breaches still involve compromised credentials.

Questions to ask your team:

- Is Multi-Factor Authentication (MFA) enforced across admin accounts, remote access, and critical business systems?
- Who currently has admin rights – and are those rights still justified?
- Are dormant or unused accounts being removed regularly?

3) Human risk and culture

Why it matters: Even strong tech fails if the culture isn't secure.

Questions to ask your team:

- When was the last time we ran a phishing simulation? How did different teams perform?
- Do staff know what a security incident looks like – and how to report it quickly?
- Do we actively reward or recognise people who flag risks or near-misses?

4) Incident readiness

Why it matters: When a breach happens, speed and clarity are everything.

Questions to ask your team:

- Do we have an Incident Response Plan, and has it been tested in the last 12 months?
- Do key execs and department heads know their role in a cyber incident?
- Do we have offline access to contact lists, vendors, and playbooks?

5) Third parties and supply chain

Why it matters: Your exposure is often their mistake.

Questions to ask your team:

- Who are our most critical suppliers from a cybersecurity standpoint?
- Do we assess their security posture regularly, beyond initial onboarding?
- Would we know – quickly – if one of our suppliers was breached?

6) Measurement and accountability

Why it matters: What gets measured gets managed.

Questions to ask your team:

- Are we tracking metrics beyond "number of attacks blocked" – e.g., dwell time, phishing click rate, or response times?
- Do we have a board-level owner for cyber risk who can translate it into business terms?
- When was the last time cyber risk was discussed at leadership level with real data?

You don't have to face cyber security alone...

At Cyber Alchemy, we believe that privacy, security and trust are a fundamental right. Every individual and organisation should be able to operate online without fear.

Jamie Kelly
CEO
EVie:
"Working with Cyber Alchemy was a fantastic experience. Their responsiveness and depth of expertise significantly aided our application's launch."

Yannick Van Der Bergen
Owner
iWebDevelopment:
"Cyber Alchemy's comprehensive testing of our main application was invaluable. Their advice greatly enhanced our security. Highly recommended."

Sam Williams
CTO
DLS Health:
"Cyber Alchemy stands out with their direct approach and hacker mindset. They're more than a provider; they're integral to our platform's integrity and overall security posture."

Your bespoke route to cybersecurity empowerment

1) **ASSESS**
A full, process-led vulnerability assessment. We will uncover any risks in your infrastructure.

2) **PROTECT**
Find peace of mind and alleviate anxiety with our dependable cyber protection.

3) **ENABLE**
We'll help you build an empowered, knowledgeable organisation, ready to prevent attacks.

If you're ready to embrace cybersecurity for your organisation, we're ready to help.

CREST | Crown Commercial Service Supplier | CYBER ESSENTIALS | CYBER RUNWAY by plexal

CYBER ALCHEMY®

ASSESS·PROTECT·ENABLE

Cyber Alchemy
Unit G1
Advanced Manufacturing Park
Brunel Way
Catcliffe
Rotherham S60 5WG

Email: sales@cyberalchemy.co.uk
Call: 0114 4000377