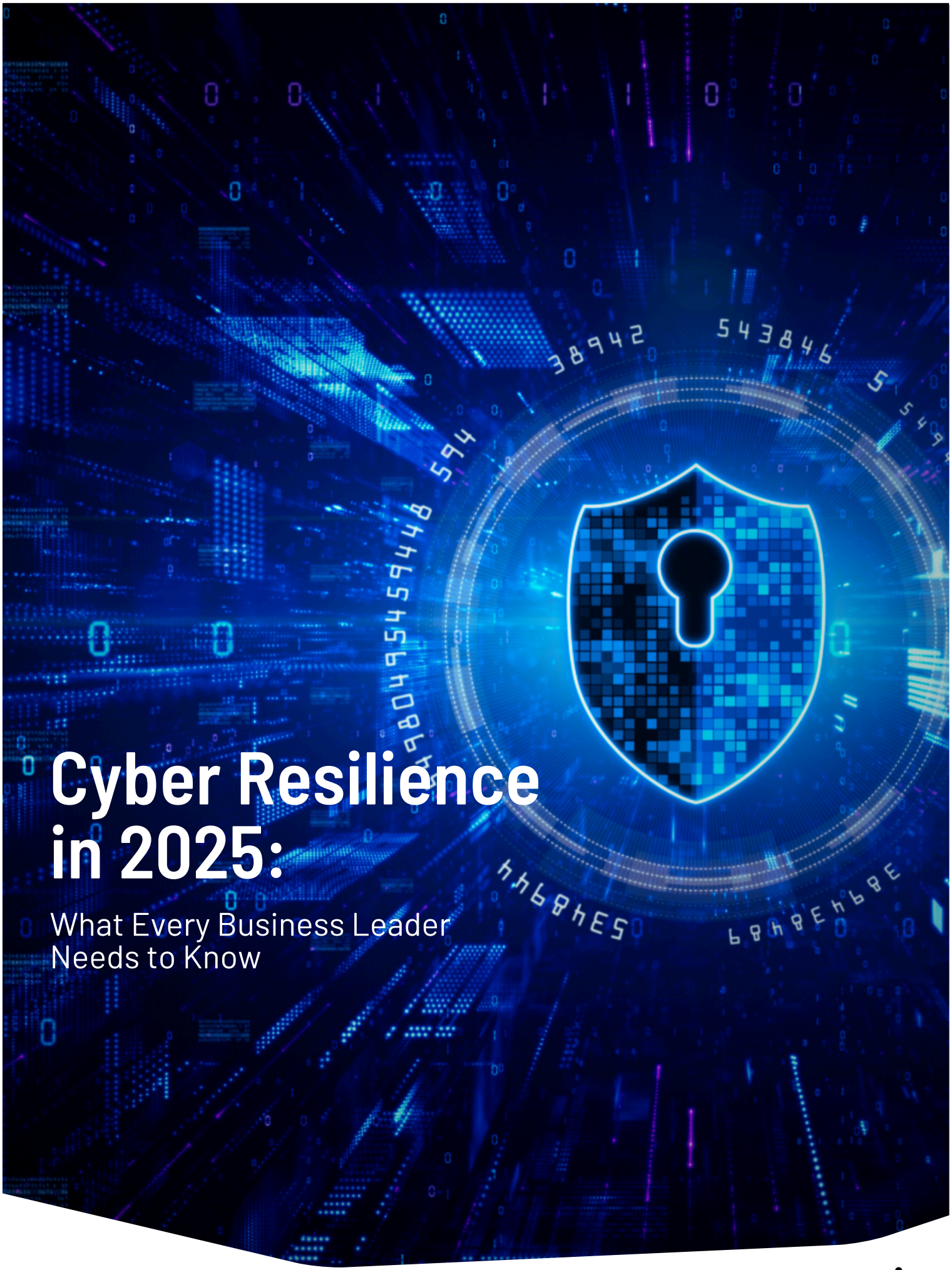


Cyber Resilience in 2025:

What Every Business Leader Needs to Know

Kytec

This guide is written for business and technology leaders who carry the responsibility for cybersecurity — and for those who would be most affected if something goes wrong.

While security vendors may have a vested interest in highlighting threats, the reality is undeniable: **attacks are more frequent, more sophisticated, and more financially damaging than ever.** Cybercrime is now the third-largest economy in the world, projected to cost over **$13.8 trillion globally in 2025.**[1]

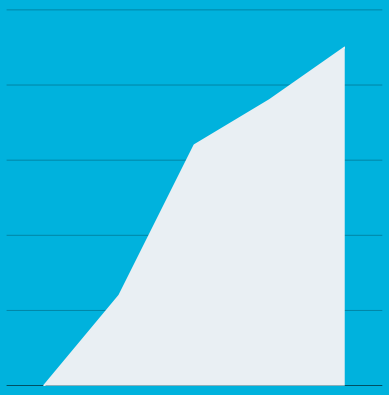
The modern threat landscape is shaped by:

- **AI-generated phishing and impersonation attacks**
- **Ransomware-as-a-Service,** lowering the barrier to entry for attackers
- **SaaS and third-party sprawl,** which creates blind spots and unmanaged risk
- **Hybrid work models** and personal device use, which dissolve the traditional network perimeter

Security breaches are rising **11% year-on-year**, and even small organisations are in the firing line.[2]

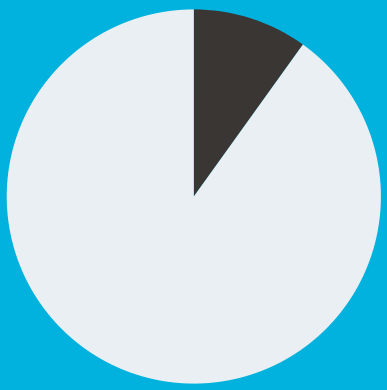
In Australia, the average cost of a breach now exceeds **$4.26M AUD**, and most companies are still underprepared.[3]

This paper highlights the most common — and most ignored — risks, outlines actionable strategies to reduce exposure, and helps security leaders take a more holistic, business-aligned approach to cyber risk in 2025.



$4.26M

In Australia, the average cost of a breach now exceeds **$4.26M AUD**



11%

Security breaches are rising 11% year-on-year, and even small organisations are in the firing line.

1. **Cybersecurity Ventures (2023).** *Cybercrime To Cost The World $13 Trillion Annually By 2025*
2. **SonicWall Mid-Year Cyber Threat Report (2024)**
3. **IBM & Ponemon Institute (2024).** *Cost of a Data Breach Report 2024*

Kytec

Perimeters Are Dead.
Identity Is the New Frontline.

The way we work has fundamentally changed. People, data, and applications now operate across office networks, home environments, and public cloud infrastructure — often simultaneously. Traditional security models that relied on physical boundaries and firewalls are no longer fit for purpose.

In today's landscape:

Workforces are mobile and distributed

Apps and infrastructure are hosted across multiple cloud platforms

Devices are often unmanaged or outside IT's direct control

This decentralisation has turned identity into the new perimeter. If an attacker gets hold of a valid login — especially one without multi-factor authentication — they can move through systems undetected.

Cybercriminals Don't Target Big Names.
They Target Easy Wins.

High-profile breaches make headlines, but they aren't the full picture. Cybercriminals aren't just chasing large enterprises anymore — **they're automating attacks at scale,** focusing on smaller targets with weaker defences.

Kytec

68% of attacks are aimed at small and mid-sized businesses

Credentials, customer data, and credit cards are harvested and sold multiple times

Social engineering and credential stuffing make it easy to break in with minimal effort

Case in Point

*A niche e-commerce business processed over **1,000 transactions** in its first few months — but it didn't realise its checkout form was vulnerable. Attackers scraped every customer's card details and sold them on the dark web. The breach wasn't discovered until credit card fraud reports began surfacing weeks later.*

Cyber Risk Is Now a Whole-of-Business Issue

Cybersecurity used to be seen as "just an IT problem." That era is over. Today, cyber risk directly affects your ability to operate, earn revenue, and retain customer trust. Accountability now spans:

- **The CEO,** for business continuity and resilience
- **The CFO,** for financial and insurance exposure
- **The CIO/CISO,** for operational and technical oversight
- **The Board,** for risk governance and compliance

The challenge?

Most organisations still face limited budgets, unclear ownership, and noisy security vendor markets. Yet inaction is a high-stakes gamble.

The Silent Breach:
100 Days of Undetected Threats

A staggering reality: *the average time to detect a breach is still close to 100 days. That's over three months where an attacker may be silently gathering intel, moving laterally through systems, or staging ransomware.*

Imagine a criminal living undetected in your home for 100 days.

Watching your behaviour. Cataloguing your valuables. Learning when you're away.

Then, they strike — and it's devastating.

This is why visibility and early detection are mission-critical. Most businesses aren't breached due to a lack of technology — they're breached because they don't know where their risks are, who has access to what, or how fast they can respond.

What This Guide Will Cover

In the pages ahead, we'll explore:

- The top attack vectors in 2025: email, endpoints, and unsecured web traffic
- The human firewall — and how to strengthen it
- A practical approach to Zero Trust, identity-first security, and layered protection
- The difference between protection and resilience
- An actionable, prioritised roadmap to improve your security posture

This isn't about hype. It's about helping you secure what matters, reduce your risk, and build confidence that your business can operate safely — no matter the threat landscape.

Kytec

Top Attack Vectors

Kytec

01

Email: Your Front Door is Wide Open

In 2025, email remains the most exploited vector in cybersecurity attacks. It's familiar, universal, and trusted — which makes it ideal for attackers. Phishing messages have become so realistic that even trained employees are vulnerable. Powered by AI, modern phishing emails mirror legitimate internal communications, often bypassing traditional filters.

For attackers, this is a numbers game. With minimal effort, they can distribute thousands of emails and wait for just one person to click. The consequences can be severe — credential theft, malware installation, unauthorised fund transfers, or internal account takeover.

90% of cyberattacks start with email [4]

80% of breaches involve compromised credentials [5]

People: The First Line of Defence

Cybersecurity is no longer just about firewalls and antivirus. The most common point of failure is still human error. A distracted staff member might click on a malicious link disguised as an invoice, calendar invite, or system notification. That's all it takes.

To strengthen this weak spot:

- Run phishing simulations to test staff reactions
- Train employees regularly with short, relevant sessions
- Promote reporting by making it easy to flag suspicious emails

Multi-Factor Authentication (MFA)

MFA prevents attackers from accessing systems even if credentials are stolen. It's essential to:

- Enforce MFA on all critical systems
- Avoid relying solely on SMS-based codes
- Apply it to both staff and third-party users

4. **Verizon (2024).** *Data Breach Investigations Report.*
5. **Cisco (2024).** *Annual Cybersecurity Report.*

Augment with Technology

AI-powered email security solutions detect anomalies and intent, flagging threats even when they appear legitimate. DNS-layer protection adds another barrier by blocking malicious sites before content loads.

Key Takeaways

- **Email is the #1** threat vector — and evolving fast
- **MFA** significantly reduces credential abuse risk
- **Awareness training and simulation are vital**
- **AI and DNS** protection strengthen defences beyond traditional filters

Email may be a daily tool — but it's also the front door into your business. Secure it accordingly.

02

Gain Deep Visibility into Traffic Patterns

In today's hybrid, cloud-first world, visibility isn't just important — it's everything. You can't defend what you can't see.

Understanding how data flows across your organisation is a critical first step in reducing risk. Are employees uploading documents to AI-powered PDF tools? Are they transferring files through consumer-grade apps like Dropbox or WeTransfer? What cloud applications are in use, both officially sanctioned and shadow IT? What types of attachments are entering and leaving your environment daily — and do you have insight into what they contain?

These aren't theoretical questions. Consider a marketing team collaborating with a freelance developer to build a new website. Large volumes of content are exchanged with an external party — often without IT oversight. Meanwhile, a public-facing platform is being built that may inadvertently expose customer data or become a soft entry point for attackers. Without visibility, there's no way to proactively manage these risks.

This is where advanced DNS-layer protection becomes essential. DNS — the digital equivalent of a phone book for the internet — translates domain names (like www.apple.com) into numerical IP addresses. Every time a user clicks a link, DNS protection acts as the first checkpoint.

Modern DNS security tools inspect web requests in real time, flagging and blocking connections to known malicious destinations — whether it's a domain linked to phishing, malware distribution, or command-and-control activity. By enforcing security at the DNS and IP layers, you prevent threats before they ever reach a device or network.

In 2025, with increasingly sophisticated cyberattacks and an explosion of SaaS usage, DNS protection is no longer optional — it's foundational.

03

Shadow IT: The Hidden Threat Inside Your Business

Shadow IT isn't new — but in 2025, it's more widespread and more dangerous than ever.

With the ease of cloud procurement and the rise of subscription-based everything, business units are now just a few clicks (and a company credit card) away from deploying powerful tools — often without IT's knowledge or approval. Marketing teams spin up CRM or automation platforms. Sales adopts third-party quoting tools. Project teams collaborate on unauthorised file-sharing apps. The intent is often good — speed, productivity, innovation — but the consequences can be severe.

Bypassing IT doesn't bypass risk. It magnifies it

Rick Orloff, former CSO at Code42, puts it bluntly:
"Shadow IT exists to bypass governance and control. But that's also what makes it one of the leading sources of insider data threats."

Consider this:
A team uploads customer data into a cloud platform that lacks encryption or doesn't meet your compliance requirements. Or an employee uses their personal credentials to sign up for a file-sharing service, exposing your organisation to a data breach or loss — especially when that employee leaves.

*Even more concerning is scale. Cisco reports that while most IT teams believe their organisation uses around **50 cloud services**, the real number **is closer to 730.**[6]*

***That's hundreds** of blind spots in your security landscape.*

50
Cloud services
(Perceived number)

730+
Cloud services
(Reported by Cisco)

6. Cisco Cloud Security Report (2024).

Kytec

Beyond the security risks, Shadow IT creates serious operational headaches:

- No central visibility into data flows or access points
- Redundant tools that dilute purchasing power and support resources
- Zero integration, leading to silos and inefficiencies
- Loss of control over data when staff leave or services go dark

In one real-world example, a mid-sized enterprise discovered it had eight separate cloud storage vendors in use — each with its own risk profile, support terms, and access gaps.

To reduce exposure and regain control, organisations need both technology and policy:

- Implement cloud access security brokers (CASBs) or SaaS management platforms to detect and control unsanctioned usage
- Regularly audit cloud traffic and subscriptions
- Educate staff on why visibility and security go hand in hand — and how rogue tools put the entire business at risk

Shadow IT isn't just a governance issue. It's a growing security blind spot — and if left unchecked, it's only a matter of time before it becomes an entry point for the next breach.

6. Cisco Cloud Security Report (2024).

04

Defending Against Ransomware: From Panic to Preparedness

Few cyber threats strike fear into IT and security leaders like ransomware — and for good reason. A single successful attack can encrypt your entire environment, lock access to critical systems, and demand a ransom (often in cryptocurrency) for the return of your own data. Business operations grind to a halt. Recovery is expensive, disruptive, and, in some cases, never fully complete.

But here's the harsh truth: ransomware isn't just a risk for high-profile enterprises. Attackers are targeting small and mid-sized businesses at scale, exploiting weaker defenses and automated scanning tools to find the fastest path to payday. It's not personal — it's profitable.

And once they're in, you're left with two options:

Pay the ransom and hope the decryption key works (with no guarantee).

Recover from backups and get back to business — quickly and confidently.

That's why modern data protection strategies are your best ransomware insurance. A well-architected backup and recovery solution ensures your data is consistently replicated, isolated, and recoverable — whether it's stored on-premises or in the cloud. With the right design, you can restore operations in as little as 15 minutes — not days or weeks.

Your mean time to restore (MTTR) becomes your resilience benchmark — and it's what separates a security event from a full-blown crisis.

One common misconception is that cloud platforms like Microsoft 365 automatically handle all backup needs. They don't. Microsoft provides geographic redundancy — not comprehensive data recovery. If files are encrypted or maliciously deleted, restoration is your responsibility.

The numbers are eye-opening:

60% of sensitive cloud data is stored in Office documents [7]

75% of that data is not backed up [8]

Without a separate backup solution in place, your business may be more vulnerable than you think.

The Bottom Line:

Ransomware isn't going away. But with robust backup, rapid recovery capabilities, and clear security policies in place, you remove the attacker's leverage — and take back control of your business.

7. **Veeam (2024).** *Cloud Data Management Report 2024.*
8. **Veeam (2024).** *Cloud Data Management Report 2024.*

05

Firewalls Are No Longer Enough

Firewalls have long been the cornerstone of enterprise security — a digital moat designed to guard the perimeter of the network. They inspect, filter, and block traffic based on predefined rules. For years, they were your first and last line of defense.

But in 2025, the threat landscape — and the way we work — has fundamentally changed.

Today's workforce is distributed. Employees work from home, co-working spaces, airports, and coffee shops. Business-critical apps live in the cloud. And data moves fluidly across endpoints, SaaS platforms, and third-party integrations. The concept of a fixed "network perimeter" has all but disappeared.

The Problem with Relying Solely on Firewalls

Firewalls still play a role — especially next-generation and cloud-delivered firewalls — but they are no longer sufficient on their own. Why?

01

They are rule-based and reactive.
Once attackers understand your firewall policies, they can design attacks to bypass them. Phishing, ransomware, and botnets are often specifically engineered to do just that.

02

They don't stop insider threats.
A firewall might keep external threats out, but it won't help if someone with internal access — like a contractor or compromised staff account — becomes the threat.

03

They don't protect identity-based access.
If someone calls the IT helpdesk claiming to be a staff member and requests a password reset, how does your team verify their identity? Firewalls can't help here — but policies like zero trust and tools like multi-factor authentication (MFA) can.

04

They don't cover direct-to-cloud traffic.
Remote users often bypass the corporate network entirely, accessing apps like Salesforce, Microsoft 365, or Dropbox directly from personal devices. This traffic never hits the firewall.

The New Security Perimeter is Identity, Data, and Context

Modern cybersecurity requires a layered, adaptive approach:

- Cloud-delivered security that follows users wherever they go
- Zero trust architecture, where no device or user is trusted by default
- MFA and strong identity controls to verify every access request
- Behavioral analytics to detect anomalies, not just block known threats
- Data loss prevention (DLP) to protect what matters most: your data

> *And importantly, your security model must be as dynamic as your business. Whether an employee is working from HQ or a hotel, using a corporate laptop or personal device, your policies need to follow them — not just defend a static perimeter.*

Firewalls still matter — but they're just one layer in a much broader security fabric. To stay secure in a perimeter-less world, you need visibility, control, and protection that travels with your users and your data, wherever they go.

06

Endpoint Security: Securing the Edge of Your Enterprise

In 2025, the endpoint is the new frontline. Laptops, smartphones, and tablets are the gateways into your business — and every one of them represents a potential entry point for attackers.

Managing these endpoints is no longer about simply rolling out a Standard Operating Environment (SOE). With hybrid work now the norm, device diversity has exploded. Staff connect from home networks, personal devices, and across regions — often outside traditional IT oversight.

The Challenge: Endpoints Are a Moving Target

- Outdated operating systems and unpatched software are among the most common vulnerabilities exploited in cyberattacks.
- Traditional antivirus solutions are no longer enough. Modern threats are faster, smarter, and constantly evolving — meaning signature-based tools often miss them.
- Relying on manual patching introduces delay and risk. Every unpatched device becomes a potential doorway into your network, and automated exploit scripts are always scanning for them.

The solution?
Automated, policy-driven endpoint management that ensures every device is secure, updated, and monitored — without relying on human intervention. Combine this with next-gen endpoint detection and response (EDR) tools that use AI and behavioural analysis to detect and respond to suspicious activity in real time.

Security Is a Supply Chain Issue

You don't operate in a vacuum — and neither does your risk. Every vendor, supplier, and partner in your ecosystem can introduce vulnerabilities.

Banks, government agencies, and large enterprises now require vendors to meet stringent security standards — often including compliance with frameworks like ISO 27001, proof of regular penetration testing, or clear policies around breach reporting and data protection.

Kytec

If your security posture doesn't meet these expectations, you may lose out on key contracts or be removed from a supplier list altogether.

Weak security doesn't just expose you — it threatens your business relationships and revenue.

Investing in strong endpoint protection and third-party risk governance is no longer optional. It's a commercial necessity.

Don't Overlook the Insider Threat

Not every breach comes from the outside. Whether it's a disgruntled employee, a former staff member with lingering access, or a well-meaning user who accidentally exposes data, **insider threats are a real and growing concern.**

Ask yourself:

- Do you have full visibility into where your sensitive data lives?
- Can you revoke access the moment an employee leaves?
- Do you have data loss prevention (DLP) and audit trails in place?
- Is your backup solution reliable enough to recover from malicious deletions?

Internal breaches can lead to lost IP, regulatory breaches, and legal action — especially if emails, documents, or customer records are deleted or leaked.

The Bottom Line

Your endpoints, your partners, and your people all form part of your risk surface. To stay secure, IT and Security Managers need an integrated approach that includes:

- Automated patching and endpoint visibility
- Real-time detection and response
- Strict access controls and offboarding protocols
- Supply chain risk assessment and compliance
- Reliable, fast recovery with backup and restoration plans

Security isn't just about keeping threats out — it's about knowing what's happening on the inside, who's connected, and how fast you can bounce back if something goes wrong.

07

Strengthening Your Human Firewall

Technology alone won't keep your organisation safe. One of the most common — and costly — vulnerabilities in your security posture is human error. In fact, 95% of cybersecurity breaches can be traced back to user mistakes.[9]

Despite the best firewalls, threat detection systems, and endpoint protection, it only takes one click on a phishing email to open the door to ransomware, credential theft, or data loss.

That's why your people are your first line of defence — and your biggest potential weakness.

Security Awareness Isn't Optional — It's Essential

For IT and Security Managers, building a strong human firewall means creating a culture of security awareness across the business. That's no small task, especially when security isn't your employees' day job. But the right mix of education, process, and reinforcement can make a major impact.

Focus on practical, high-risk behaviours:

01

Teach staff how to identify phishing and social engineering attempts — and what to do when something looks suspicious.

02

Encourage a "check with IT first" culture before anyone installs, subscribes to, or purchases cloud apps, storage, or software.

03

Ensure all devices — PCs, phones, tablets — are kept up to date with the latest security patches.

04

Mandate and promote multi-factor authentication (MFA) as a non-negotiable standard.

Prioritise Security Education for Strategic Users

Not all users carry equal risk. Some employees have access to sensitive financial controls, intellectual property, or customer data — making them high-value targets for attackers. These "strategic users" need an elevated level of security awareness and control.

9. Verizon Data Breach Investigations Report (DBIR) 2024

Start by identifying:

- **Who controls budgets and payments?**
  (CFO, Accounts Payable, Procurement, Marketing)
- **Who handles sensitive data or intellectual property**
  (Engineering, R&D, Legal, Customer Service, HR)

Once identified, apply tailored policies:

- Additional MFA requirements
- More frequent awareness training
- Access monitoring and behavioural alerts
- Restrictions on unsanctioned software or cloud usage

> *This targeted approach not only reduces risk — it makes your awareness efforts more effective by focusing on the people who matter most.*

The Bottom Line

Your security architecture is only as strong as the people using it. Empower your team to be vigilant, informed, and proactive — and turn your weakest link into your strongest defense.

In today's landscape, security is everyone's responsibility — but it starts with you.

08

Multi-Factor Authentication: Still Critical, But No Longer Bulletproof

By now, every security leader knows that MFA is table stakes. But in 2025, simply enabling MFA isn't enough — not when adversaries are actively developing techniques to bypass it.

MFA fatigue attacks, SIM swaps, man-in-the-middle phishing proxies, and social engineering are all being used to sidestep legacy MFA methods. The rise of these techniques has shifted the conversation: ***it's no longer about whether you use MFA, but how intelligently and resiliently it's implemented.***

MFA in a Modern Threat Landscape:

- Push notification abuse is now a common tactic. Repeated approval prompts wear down users — and eventually, many just click 'approve.'
- Legacy methods like SMS are increasingly vulnerable to interception and SIM-jacking.
- Basic MFA gives a false sense of security if it's not backed by contextual policies or device verification.

What Advanced MFA Looks Like in 2025:

- Phishing-resistant authentication (e.g. FIDO2, passkeys, certificate-based auth)
- Risk-based adaptive access (evaluating device health, IP reputation, geolocation anomalies, and behavioural biometrics)
- Integration with endpoint compliance tools (ensuring only patched, managed devices are granted access)
- Continuous authentication — not just one-time validation at login

Why It's Foundational to Zero Trust

Zero Trust assumes breach. That means identity verification can't be a single point in time — it must be continuous, dynamic, and risk-aware.

Modern MFA should:

Automatically block access from non-compliant or high-risk devices

Dynamically step up authentication based on real-time context

Work seamlessly across all access points — cloud, on-prem, hybrid, and mobile

> *"MFA is still one of the most effective controls we have — but only when implemented as part of a layered, adaptive, and Zero Trust-aligned architecture."*
> ***— Australian Cyber Security Centre, Essential Eight***

Bottom line:

If your **MFA strategy** hasn't evolved in the last **12–18 months**, it's time to revisit it. Attackers have moved on — and your defences need to keep pace.

Five Key Takeaways for Building a Resilient Security Strategy

Kytec

1. Benchmark Your Current State — Start with a Security Assessment

You can't secure what you can't see. Before improving your security posture, you need a clear understanding of where you stand today. That means visibility into:

- What traffic is flowing across your network
- Which cloud applications and third-party services are in use
- Which devices are accessing your environment — and how they're being secured

This is where a Security Assessment becomes essential. A credible, independent assessment provides a structured, unbiased view of your current vulnerabilities, policy misalignments, and areas of exposure — often using real-time monitoring over a defined period (e.g. seven days).

A good assessment doesn't just identify technical issues — it benchmarks your security maturity across people, process, and technology. It provides the clarity needed to make informed decisions, justify investments, and demonstrate due diligence to executive stakeholders.

A robust security strategy starts with visibility — and visibility starts with a proper assessment.

Whether you're just beginning to build out your cybersecurity strategy or refining an existing one, this step sets the foundation for everything that follows.

2. Know Your Risks — and What They Could Cost You

Cybersecurity isn't just an IT issue — it's a business issue. Assess your risks in terms of business impact, not just technical severity.

Ask the tough questions:

- **What's the immediate and long-term fallout of losing customer data?**
- **What's the financial impact of a 24-hour outage on your e-commerce platform?**

What would a ransomware attack cost you — in ransom, downtime, and reputation?

How much should you invest now to avoid larger losses later?

Understanding the risk-to-impact ratio helps justify security spend and prioritise action. Risk is unavoidable — but unmanaged risk is unacceptable.

3. Build a Strategy, Not Just a Shopping List

Once you've benchmarked your current environment and mapped key risks, it's time to build a plan — what you'll do, when, and why.

Shockingly, over **77% of** organisations still don't have a cybersecurity response plan,[10]

Your security roadmap should:

- Prioritise based on risk, not hype
- Balance cost vs. coverage across multiple financial years
- Avoid siloed, piecemeal solutions in favour of a cohesive, architectural approach
- Focus on capabilities and outcomes, not just product names
- Where possible, consolidate vendors to benefit from shared threat intelligence across a global customer base

And remember: a phased rollout is okay. In fact, it's often smarter and more sustainable.

Communicate Strategically

Security isn't just a technical challenge — it's an organisational responsibility. That means:

- Identify and brief your key stakeholders early — especially those who control budgets or are impacted by breaches
- Keep your Board informed — directly or via senior leadership — to align with risk governance obligations
- Provide regular, meaningful updates to business units: what's being done, why it matters, and how their data is protected

10. IBM X-Force Threat Intelligence Index 2024

The business wants assurance, not jargon. Speak their language and show how security supports business continuity, compliance, and customer trust.

Empower Your People — Build a Human Firewall

Technology alone can't stop phishing, credential theft, or social engineering. Your employees are both your greatest risk and your greatest asset.

Invest in building security awareness and positive behaviour:

- Train staff to recognise threats like phishing emails and suspicious activity
- Create a culture where reporting incidents is encouraged, not punished
- Reinforce the importance of security hygiene — from MFA to device patching

Focus especially on high-risk users — those with access to finances, sensitive IP, or critical infrastructure. Tailored education and policy controls can dramatically reduce your exposure.

"A robust security system contains more than just hardware or software; there must always be a human element — a 'human firewall [11]
— Infosec Institute

Final Thought:

Cybersecurity is not a set-and-forget project — it's a continuous journey. With the right strategy, empowered people, and aligned stakeholders, you can build a security posture that is not only technically strong, but also business resilient.

11. **Infosec Institute (2024).** *Building a Human Firewall.*