



Making cyber resilience a reality

How SMBs can supercharge their security posture



Cutting through the noise

By Andy Winters, Director of MSS Operations at Ekco

For small and medium-sized businesses, cybersecurity defence can feel like a constant uphill battle. Every day brings fresh, and potentially devastating, risks - from phishing scams and ransomware to vulnerabilities in software or human error.

But what makes things even harder for organisations is the pressure to stay secure with limited time, budget, and in-house expertise.

Tech stacks are getting ever more complex. The average small to medium-sized business (SMB) runs 58 applications¹, while most SMBs have evolved a sprawl of on-prem systems, cloud apps, and remote work setups.

The advice out there often feels too generic to be useful.

The truth is, most SMBs aren't lacking in care or effort. They're simply overwhelmed. Siloed tools don't talk to each other. The cybersecurity talent gap keeps growing and the advice out there often feels too generic to be useful.

This eBook is designed to cut through the noise. It's for business and IT leaders who want practical, real-world insights into what works - and what doesn't - when it comes to building a more resilient security posture. We'll explore the risks, the realities, and the steps you can take to protect your business without breaking the bank or burning out your team.

Security doesn't need to be perfect. It needs to be effective - and it needs to work for you.

Let's get into it.



The average small to medium-sized business (SMB) runs 58 apps.

¹SMBs at Work 2024 Report - Okta

Why SMBs are feeling the pressure

Ransomware. AI-generated attacks. Phishing and social engineering. Threats from the supply chain, insider risks, zero-day vulnerabilities - the list keeps growing. For many small and medium-sized businesses (SMBs), the cyber threat landscape has become too complex to manage alone.

In the past, smaller businesses might have flown under the radar. But today, they're seen as prime targets. In 2024, nearly 60% of small businesses and 70% of medium-sized firms reported experiencing a breach.² For one in five, the fallout was severe enough to threaten the future of the business.³

Why is this happening? Because while threats have grown in sophistication, the ability and capabilities of SMBs to defend themselves hasn't kept pace.

Most lack the internal expertise to manage complex security tools or make sense of threat intelligence. Hiring skilled professionals is tough - demand far outweighs supply with

ever increasing salary costs. On top of that, the financial reality of achieving robust cyber defences and resilience is stark: SMBs can't justify the kind of cybersecurity budgets large enterprises take for granted.

And it's not just a people or budget problem. Many SMBs now operate in mixed environments - on-prem, Software as a Service (SaaS), cloud - which creates a fragmented and often unclear picture of their own risk exposure. When systems don't connect and visibility is limited, it's all too easy for threats to slip through the cracks.

These barriers - cost, capability, and complexity - leave many SMBs stuck in reactive mode. Security becomes a patchwork of point solutions rather than a coherent, strategic approach.

But while the challenge is real, it's not impossible. With the right partner, tools, and mindset, resilience is within reach.

In the rest of this eBook, we'll show how.



In 2024, nearly 60% of small businesses and 70% of medium-sized firms reported experiencing a breach.

² <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024>

³ <https://www.hiscox.co.uk/sites/default/files/documents/2023-10/Cyber-Readiness-Report-2023-UK.pdf>

Strengthening your defences

“When... not if.” Every business needs to be prepared for the worst.

In June 2023, a UK-based logistics company that had been in business for over 150 years was hit by a ransomware attack. Despite having reasonable cybersecurity systems in place, the company - Knights of Old - was knocked sideways by the attack. The company was not just financially solvent, it was well-known: its logistics vehicles were a common sight on the UK's roads. It employed 700 people and delivered annual revenues of over £50m. This was no fragile, failing business.

But the ransomware attack was too much for the company to withstand. The disruption to its business and income meant that in September 2023, the whole company ceased trading and shut down for good.

The Knights of Old story is a painful lesson to every SMB, a reality check for today's security landscape.

Cyberattacks are no longer rare events - they're a constant threat. And they have the power to take your company down. For small and medium-sized businesses (SMBs), that's an uncomfortable truth. Attackers are opportunistic. They don't always go after the companies with the most to lose - they target the ones with the weakest defences.

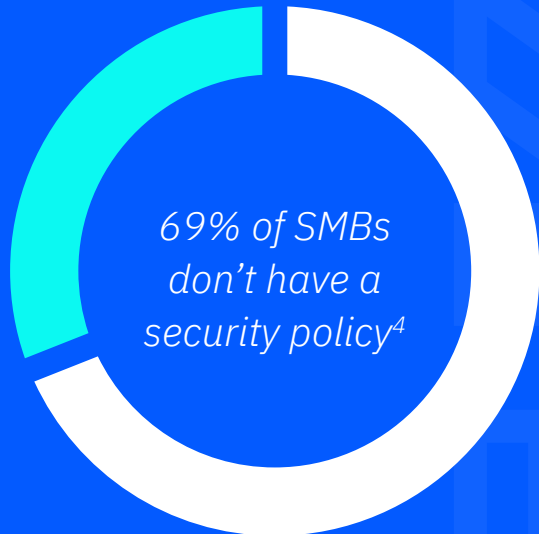
So, how do you protect your business when the risks are everywhere and always changing?

The answer lies in building a clear, balanced security posture - one that doesn't just focus on tools and technologies, but on outcomes. That means understanding your environment, protecting what matters, spotting threats quickly, and recovering fast if something slips through which, in today's threat landscape, is inevitable.

Here, we explore the five pillars of a modern security strategy, tailored to the challenges SMBs face today.



SMBs can be fined 4% of annual revenues under GDPR



69% of SMBs don't have a security policy⁴

⁴<https://www.infosecurity-magazine.com/news/uk-smes-lack-cybersecurity-policy/>



1. Identify

Understand what you have and where the risks lie.

You can't protect what you don't know. That's why the first step in strengthening your defences is visibility. This means taking stock of your assets - data, devices, users, applications - and mapping out your environment, including remote and cloud-based systems to fully understand your attack surface and any weaknesses. Know your assets and understand your risk.

The SMB priority:

Most smaller businesses operate with limited visibility. Shadow IT, unmanaged devices, BYOD and legacy systems are common. Investing in automated asset discovery and vulnerability management tools, combined with regular audits and governance, is a great place to start.



What you can do:

- Maintain an up-to-date inventory of assets and grade them against business criticality.
- Understand your attack surface and any vulnerabilities or gaps within your systems that provide attackers opportunities.
- Perform regular security assurance testing (Penetration Testing) against external systems and services. Ensure you remediate and rectify findings quickly.
- Understand data locations and classify data based on sensitivity (ie. customer finance, Intellectual Property, Personally Identifiable Information (PII), etc.).
- Identify dependencies across systems and applications.
- Look for gaps in coverage (especially in cloud and SaaS apps).

2. Protect

Put proactive measures in place to stop attacks before they start.

Protection is where many SMBs focus first - and rightly so. Firewalls, endpoint protection, multifactor authentication, encryption - these are your basic defences. But too often, businesses rely on individual tools without a broader strategy. The result is a patchwork setup with hidden blind spots.

The SMB priority:

Start with the essentials: strong access and identity controls and secure configuration by design, with regular maintenance, patching and software updates. If your team uses the same passwords across systems or skips updates, that's your first risk to fix. The majority of cyber breaches commence with identity or vulnerabilities as the initial attack vector.

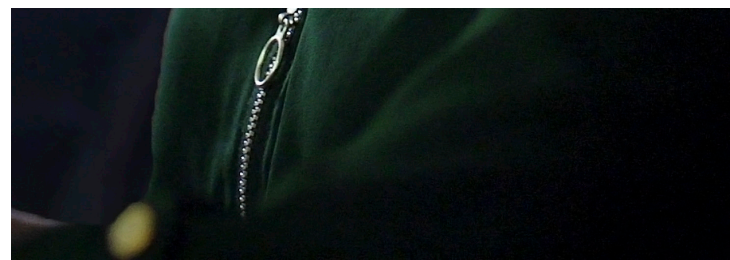


What you can do:

- Enforce strong password policies and MFA everywhere – no exceptions!
- Protect and monitor privileged and administrative accounts (Domain Admin, Server Admin, Local Admin, Root Accounts) with Privileged Access Management (PAM) policies and tools, ensuring least privilege necessary to fulfill role responsibilities.
- Use Endpoint Detection and Response (EDR) tools. Antivirus alone will not provide the right level of protection against today's cyber threats.
- Apply security patches and updates promptly - waiting a month until the next scheduled patching won't suffice against the speed of today's adversaries.
- Train, educate and test all employees regularly to avoid phishing and social engineering traps. Education is critical to cyber defence.
- Train helpdesk and IT support staff to avoid helpdesk social engineering tactics now used by many adversaries to gain initial access.



The majority of cyber breaches commence with identity or vulnerability as the initial attack vector.





3. Detect

Spot threats before they become major incidents.

Detection is about early warning. The faster you spot a breach or anomaly, the faster you can contain it. Unfortunately, many companies only realise there's a problem when it's too late - when systems go down or customer data is leaked.

The SMB priority:

Even basic detection can make a huge difference. Email alerts for login anomalies, tools that flag suspicious activity, and security monitoring services help you catch things before they escalate.



What you can do:

- Use monitoring tools like Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) that alert unusual access patterns or behaviour across your environment and endpoints.
- Ensure you can monitor and alert on identity basics like failed login attempts, unusual access location attempts and elevation or changes of access privileges.
- Strongly consider an outsourced Managed Detection and Response (MDR) service providing 24/7 monitoring to fill skill gaps and ensure you get the correct visibility and monitoring. Attackers don't sleep, neither can your business when it comes to monitoring threats.
- Review logs regularly - or better yet, automate the review.

Strongly consider an outsourced Managed Detection and Response (MDR) service to fill skill gaps.

4. Respond

Act fast to limit damage when something goes wrong.

Once a threat is detected, what happens next? That's where the business response comes in. A strong cyber incident response plan helps reduce downtime, limit financial and reputational damage, and avoid the chaos that often follows an attack.

The SMB priority:

Have a simple, clear plan that is not only documented but reviewed and rehearsed regularly - a plan that hasn't been rehearsed and communicated effectively will often lead to chaos in a real life scenario. Which person or team performs response plan activities? Who needs to know about the incident? Who makes decisions? Who communicates? What systems need to be shut down, isolated, or restored?



What you can do:

- Create a cyber incident response plan - even a basic one. These are available online providing guidance through the NCSC to aid SMB organisations.
- Rehearse the Cyber Incident response plan regularly ensuring that lessons learned are documented and captured.
- Define key roles and responsibilities in advance ensuring there are no single points of failure.
- Have a known and ready alternative communication method outside of your business systems. How will you communicate in a crisis if your primary internal tools are compromised or unusable?
- Have contact information for key stakeholders (internal and external) ready to go in the event of an emergency. Storing these only on your internal systems only will cause a plan to fail.





5. Recover

Get back to business as quickly and safely as possible.

Resilience means more than defence - it's about bouncing back. Recovery is the final piece of the puzzle, and arguably one of the most important. A strong recovery capability limits disruption and restores confidence after a security event.

The SMB priority:

Backups are essential, but not enough alone. You also need to regularly test those backups or failover capabilities, know how long recovery will take, and understand what data you'll lose (if any).



What you can do:

- Use secure, offsite, or air gapped immutable backups that can't be tampered with.
- Have multiple backup copies available and follow best practice for recovery by following the 3-2-1-1 methodology as closely as you can. Three copies of data, two media storage types, one offsite, and one immutable and air gapped.
- Test your recovery process regularly - restore test files, systems and simulate outages or failover capabilities regularly.
- Document recovery steps clearly for all key systems and services. Ensure these are stored offline.
- Prioritise recovery for business critical systems (e.g. finance, customer data, email).

Test your recovery process regularly - restore test files, systems and simulate outages.

Bringing it all together

No single tool or policy will make your business secure overnight. But by strengthening each of these five areas - Identify, Protect, Detect, Respond, and Recover - you create a solid, adaptable foundation.

You also avoid the all-too-common trap of reactive security. Instead of waiting for something to go wrong, you prepare in advance. That preparation could be the difference between a minor incident and a major disruption.

At Ekco, we specialise in helping SMBs build this kind of resilience. Whether you need support across the board or help plugging specific gaps, we offer practical, tailored solutions that grow with your business.

*Because real-world security
isn't about perfection.
It's about preparation.*





The cost of control

High personnel costs. Expensive technology. Infrastructure upgrades. Ongoing training. The costs just keep on coming. How can you keep costs under control?

For many SMBs, building a full in-house cybersecurity function isn't just challenging - it's financially out of reach.

Security is no longer a one-time investment. It's an ongoing cycle of monitoring, updating, and responding to ever-changing threats. That means finding and keeping skilled professionals in threat detection, cloud security, compliance, and incident response - roles that are in high demand and short supply.

Even with the right people in place, the tools they need - endpoint protection, threat intelligence, 24/7 monitoring platforms, backup systems - come with heavy licensing and setup costs. Add to that the need for secure infrastructure, integrations, and compliance management, and the numbers climb fast.

Then there's the risk. Many SMBs spread their internal teams too thin, asking IT staff to juggle user support, operations, and security. That increases the likelihood of missed alerts or slow responses and even small delays can lead to big consequences.

The truth is: owning everything isn't necessary. What matters is having access to trusted protection that works.

Cybersecurity doesn't have to cost the earth. With the right support, you can stay protected, compliant, and confident - without going it alone.

*Security is no longer
a one-time investment.
It's an ongoing cycle.*

Security for the real world

Cyber threats are evolving fast - and for many small and medium-sized businesses, keeping up feels impossible. From ransomware and phishing to insider risks and compliance demands, today's challenges call for more than just tools and technology. They call for real expertise, practical solutions, and a partner who understands your world.

With all that in mind, it's not surprising that SMBs are turning to outside help. Rather than building up their own capabilities, many are looking to Managed Security Service Providers (MSSPs).

Not all MSSPs are alike

While many claim to offer everything that SMBs need, the reality can be very different.

That's where Ekco comes in.

With Ekco, SMBs get everything they need to safeguard their operations. They get deep technical expertise and a full suite of security services, all delivered at a competitive price point.

We help growing businesses take control of cybersecurity - without overwhelming their teams or budgets. Whether you have some in-house capability or are starting from scratch, we act as an extension of your business.

From ISO to CREST, we're accredited by some of the world's most prestigious organisations



Ekco is certified to ISO's world-class information security standard.



Our Security Operations Centre (SOC) is CREST approved.



Ekco is a Cyber Essentials Certified provider.



With Ekco, SMBs get deep technical expertise and a full suite of security services, all delivered at a competitive price point.



Our team delivers a full range of managed security services, including:

- Managed Extended Detection & Response (MXDR)
- Managed Detection & Response (MDR)
- Vulnerability and Attack Surface Management
- Cyber Incident Response
- Managed Threat Intelligence
- Backup and Disaster Recovery
- Patching and Remediation
- Policy and Compliance support

Our 24/7 security operations team works behind the scenes to keep you safe, spot risks early, and respond fast when something goes wrong. We help you understand your risks, improve your defences, and bounce back quickly - **so you stay focused on what matters most: running your business.**

|| *We don't just provide tools.*
|| *We provide confidence and expertise.*

Ready to strengthen your defences?

Talk to our team today to see how we can help you build cyber resilience, simplify security, and stay one step ahead of threats.

Visit **ek.co/security** or get in touch at **info@ek.co**



✉ info@ek.co

🌐 www.ek.co

☎ +44 (0)330 135 8792

📍 106 Saxon Gate, Milton Keynes