spector

State of Cybersecurity

December 2025

Contents

Navigating Digital Risk: An SME Guide to Cyber Security in Late 2025

Part 1: The Cyber Landscape in Late 2025

The cybersecurity environment is shifting rapidly. For Small and Medium-sized Enterprises (SMEs), it's crucial to understand that the threats are no longer random—they are organized, sophisticated, and often automated. Criminals have identified SMEs not just as targets, but as highly profitable ones due to smaller security budgets and higher potential for human error.

Key Trends Shaping Your Risk Profile

Trend	The Business Impact
1. Exponential Crime Growth	Organized cybercrime groups view SMEs as soft targets with valuable data and weaker defences than large corporations. Attacks are becoming cheaper and easier to launch, increasing the volume your business must repel. The consequence is a higher probability of becoming a direct victim.
2. AI is Accelerating Attacks	Artificial intelligence (AI) is used by hackers to generate highly convincing, personalized phishing emails, find software vulnerabilities faster, and automate the most complex parts of an attack. This means your employees face more sophisticated trickery, eliminating the old giveaway signs like poor spelling or grammar.
3. Cloud Misconfiguration Exposure	The rapid shift to cloud services (like Microsoft 365 or Google Workspace) often results in security settings being left in their default, less-secure state. This creates easy, open doors for attackers, turning your convenient cloud storage into an unintentional public data dump.
4. Compliance and Regulatory Pressure	New laws like NIS 2, GDPR, and the upcoming DORA (Digital Operational Resilience Act) mean that failing to protect data can lead to substantial fines, regardless of your company size. The regulatory burden is moving down the supply chain, requiring better documented defence.
5. Supply Chain Demands	Larger clients and partners are now requiring their suppliers (SMEs) to meet strict cybersecurity standards (like ISO 27001 or SOC 2). Your security posture directly affects your ability to win new contracts and maintain business relationships.

6. Onerous Insurance Requirements	Cyber insurance is increasingly difficult to obtain. Insurers now demand mandatory security controls, such as Multi-Factor Authentication (MFA) and immutable backups, before they will provide coverage. Failure to meet these minimum standards can void your policy entirely when an incident occurs.

Who is Being Targeted?

Cybercrime is not industry specific. While certain sectors hold high-value data, modern attacks cast a wide net:

Sector	**Percentage of Attacks**	**Risk Factor**
Education	21%	Contains large volumes of personal and student data, often relies on aging or under-managed infrastructure.
Healthcare	17%	Highly sensitive medical and financial patient records (PHI), which sell for a high price on the dark web.
Technology	12%	Often used as a gateway for supply chain attacks by compromising software or managed service providers.
Government	11%	Data related to citizens and internal operations, usually targeted for political or espionage motives alongside financial gain.
Manufacturing	9%	Operational technology (OT) systems and unique intellectual property (IP) like designs and proprietary formulas.

The Bottom Line: Organised crime groups like **RansomHub, Lynx, and Akira** are motivated by profit and target the path of least resistance. If you store data, you are a target, and your size is now seen as an advantage for the attacker.

Part 2: The Adversary and Their Tactics

To defend your business, you need to understand the few common steps nearly all hackers follow. Every major threat below is just a different flavour of these three steps.

The Simplified Model of How Attacks Work

Security experts use a big framework called MITRE ATT&CK that maps how attackers operate—from the first contact to the final ransom note. We simplify that idea into three core phases to ensure we have controls at each stage, stopping attacks early and limiting damage if something slips through.

Phase	Hacker's Goal	Common Tactics	Failure Consequence
1. Get In	Gain initial entry to the network or a key account.	Trick someone (phishing, fake login pages, phone scams) or break in through a weak point (unpatched system, bad password, exposed remote access).	Failure to stop here means the attacker is inside your network and establishing persistence.
2. Move Around & Take Stuff	Explore the environment to find and collect valuable assets.	Use stolen accounts to explore systems and files; find finance systems, email, client data, file shares, and backups.	Failure to stop here means the attacker has your sensitive data and knows where your backup vault is.
3. Cash Out / Cause Impact	Achieve the financial objective or cause maximum disruption.	Encrypt data and demand ransom; change bank details on invoices; steal data and threaten to leak it (double extortion); or quietly use access for long-term fraud.	Failure to stop here means significant financial loss, operational downtime, and reputational damage.

The Most Current Threats Facing SMEs (in Plain English)

Threat 1: Phishing & Advanced Email Scams (incl. MFA Fatigue)

- **What it is:** Messages pretending to be from a trusted source (CEO, bank, Microsoft) to make staff click a link, enter a password, or approve a login.
- **Why it's big now:** Phishing delivers most malware. Attackers use highly convincing emails and **MFA "fatigue" attacks** (bombarding a staff member with approval prompts until they click "Approve" just to make it stop). They also use **lookalike**

domains (e.g., spect0r.ie instead of spector.ie) which are nearly impossible to spot without close inspection.

- **Key Mitigations for SMEs:**
  - **Email Security:** Use business email filtering to catch malicious links; turn on anti-phishing features in M365/Google Admin to alert on internal impersonation.
  - **Strong Identity Controls: Enforce MFA for all remote access and email.** This is the primary defence against stolen passwords. Use a password manager and ban password reuse.
  - **Process:** Use **Out-of-band checks** for money movement: any change in bank details must be confirmed via a *known* phone number, never by replying to the email.

Threat 2: Ransomware & Data Extortion

- **What it is:** Malicious software that encrypts your files and systems. Attackers demand a ransom; they also often steal data first and threaten to leak it (**double extortion**), adding extreme pressure to pay.
- **Trends:** Ransomware incidents are significantly increasing, and Ransomware-as-a-service allows less-skilled criminals to launch serious attacks using rented tools.
- **Key Mitigations for SMEs:**
  - **Backups that Actually Work:** Follow the 3–2–1 rule (3 copies, 2 types of media, 1 offline/immutable). This ensures you can restore operations without paying the ransom. Test restores at least quarterly.
  - **Patch and Harden:** Keep servers, firewalls, and VPNs patched. Crucially, lock down remote access (RDP, VPN) immediately and protect it with strong, phish-resistant MFA.
  - **Endpoint Protection:** Use modern EDR/XDR or next-gen antivirus, which can detect and stop suspicious activity before encryption begins. Restrict admin rights for general staff.

Threat 3: Business Email Compromise (BEC) & Invoice Fraud

- **What it is:** Attackers impersonate a business account (MD, FD, supplier) and instruct staff to transfer money or change bank details. It caused billions in losses globally, exploiting human trust and process gaps.

- **Impact:** BEC relies on social engineering, meaning it often bypasses technical defences entirely, resulting in direct financial loss that is hard to recover.
- **Key Mitigations:**
  - **Lock Down Email:** Enforce MFA, enable impossible travel alerts, and use conditional access rules to detect strange login patterns.
  - **Financial Controls: Dual approval** for all large or unusual payments. Call-back verification for new bank details or urgent transfers—this must be mandatory policy.
  - **Domain Protection:** Implement DMARC, SPF, and DKIM to reduce email spoofing (ask your IT provider to manage these technical acronyms).

Threat 4: Supply Chain & Vendor Compromise

- **What it is:** Criminals attack your trusted third parties (IT suppliers, software vendors, logistics partners) and use their established access to pivot into your environment.
- **Trends:** SMEs are often collateral damage when a larger vendor is hit. Examples include attacks against Managed Service Providers (MSPs) or widely used payroll software.
- **Key Mitigations:**
  - **Vendor Risk Basics:** Keep a list of critical suppliers. Ask them about their MFA, backups, and recognized certifications (ISO 27001, Cyber Essentials). Treat their access as your own risk.
  - **Limit Trust:** Give suppliers only the minimum access they need, and only when needed. Use per-user, logged access for remote support (avoid generic "support" accounts).
  - **Monitor and Segment:** Use Network Segmentation so a vendor tool compromise cannot expose your entire internal network, limiting the blast radius of an attack.

Threat 5: Cloud & SaaS Misconfiguration (M365, Google, CRM)

- **What it is:** Attackers exploit weak settings, public links, overly broad sharing, or poor access control within your cloud applications (M365, CRM, HR tools), rather than hacking the cloud provider itself.
- **Common Issues:** Over-permissive sharing settings ("Anyone with the link can view"), dormant accounts still active, or Global Admin accounts without MFA.

- **Key Mitigations:**
    - **Secure-by-Default:** Review M365/Google security baselines. Disable legacy protocols (like POP/IMAP) and require MFA for all cloud admins.
    - **Access Hygiene:** Quarterly review of user and admin accounts; remove dormant users immediately. Implement "least privilege," meaning staff cannot browse folders they don't explicitly need for their role.
    - **Data Sharing Controls:** Tighten external sharing. Use expiry dates and restricted locations for highly sensitive data, rather than leaving it in generic team drives.

Threat 6: Website & Application Attacks

- **What it is:** Attacks on your public website, web apps (client portals, e-commerce), or APIs to deface sites, steal data, or inject malicious code.
- **Examples:** Exploiting common vulnerabilities in Content Management Systems (CMS) like WordPress or its associated plugins, or injecting scripts that skim customer credit card data.
- **Key Mitigations:**
    - **Treat Websites as Critical:** Keep CMS, themes, and plugins fully patched. Restrict admin access, use MFA, and disable unused admin accounts.
    - **Front-Door Protection:** Use a Web Application Firewall (WAF) and DDoS protection via your host or a provider like Cloudflare. This acts as a protective shield for your site.
    - **Security Testing:** Regular vulnerability scans on public apps (at least annually) and after major code changes to proactively find and close security holes.

Threat 7: Human Error & Insider Risk

- **What it is:** Mistakes (emailing the wrong file, misconfiguring access, losing a laptop) or malicious insiders (disgruntled staff stealing or sabotaging systems).
- **Impact:** Often results from over-permissive access and a lack of monitoring. A **no-blame culture** is vital here, as it encourages prompt reporting, which minimizes the damage and recovery time.
- **Key Mitigations:**

- **People:** Clear, short policies on acceptable use and data handling. Regular awareness sessions in plain language, emphasizing the consequence of the mistake, not the person.
- **Access & Monitoring: Role-based access**; remove access immediately when staff leave. Basic alerting for unusual bulk file access.
- **Devices: Encrypt all laptops**; enable remote wipe on mobiles using Mobile Device Management (MDM).

Part 3: The Action Plan

Your Top 10 Control Checklist for SMEs

This checklist provides a powerful one-page strategy to stop the majority of the threats listed above.

#	Control	Why This Matters
1.	**MFA on Everything:** MFA on email, VPN, and admin accounts. No exceptions.	Stops 80% of all account takeover attacks, even if the password is stolen.
2.	**Continuous Training:** Phishing & cyber awareness training at least twice a year.	Turns your employees into your first line of defence against social engineering.
3.	**Managed Endpoint Protection:** Managed endpoint protection (EDR) on all devices.	Detects subtle malicious behaviour on devices *before* it becomes a full ransomware incident.
4.	**Patching Discipline:** Regular patching for servers, endpoints, firewalls, VPNs, and web apps.	Closes the known vulnerabilities that hackers exploit for easy entry.
5.	**Tested Backups:** Tested backups with at least one offline/**immutable** copy (**3-2-1 rule**).	Your ultimate insurance policy against ransomware; guarantees business continuity.
6.	**Financial Controls:** Strong financial controls (dual approval, call-back verification for new bank details).	Prevents catastrophic losses from Business Email Compromise and invoice fraud.
7.	**Cloud Hardening:** Secure-by-default cloud configuration (M365/Google hardening; disable legacy protocols).	Reduces the attack surface of your most used, public-facing applications.
8.	**Vendor List:** Vendor/supply chain list with basic security expectations (e.g., they must use MFA).	Manages the external risk that comes through trusted third parties.
9.	**Monitoring:** Logging & monitoring (or a managed SOC/MDR service) to spot unusual activity early.	Allows you to catch attackers in Phase 2 (Move Around) before they get to Phase 3 (Impact).

10.	**Incident Plan:** A short, printed incident response plan with key contacts (who to call, what to disconnect).	Saves critical hours and avoids panic when a crisis actually hits.