

Cybersecurity 2025:

What Every Business Needs to Know



Cybersecurity 2025

What Every Business Needs to Know

Immediate Takeaways

- **Cyber attacks are rising fast** and are now one of the **biggest risks** facing any business in 2025.
- Most attacks now come through **suppliers or technology partners** — your business is only as safe as the **weakest link** in your chain.
- **Simple, low-cost steps** (like strong passwords, updates, multi factor authentication and data backups) will help mitigate against most attacks.
- A **short outage or data breach** can create **major financial stress** for small and mid-sized organisations.
- **AI makes attacks easier** for criminals — but also gives businesses **powerful tools to spot danger earlier**.
- You need a **clear plan** for what to do in a **cyber incident before it happens**.

Introduction – Cybersecurity now a day-to-day business risk

Ransomware, data theft and supply chain attacks are rising worldwide. Small and mid-sized organisations (SMEs) now face the same attacks as large global companies, but often without the resources to recover quickly. This Bulletin explains the current risks in clear language, highlights real incidents from the past year, and sets out the practical steps leaders should take now.



1. What's Happening? A Fast-Changing and Growing Threat



36 billion

Nearly **36 billion** records were breached worldwide in 2024.



4.9 million

The average cost of a data breach reached **\$4.9 million**.



over 1/2

Ransomware **hit over half** of all organisations surveyed.









4,000%

Phishing (fake emails/messages) increased by more than **4,000%** in two years.

Criminals have become smarter, using fake emails, impersonation and scams to trick staff. Global conflicts have also fuelled new tools that are cheap and easy to use, meaning almost anyone can launch an attack. SMEs are often hit hardest: even a day or two of downtime can disrupt operations, damage customer relationships and strain cash flow.

2. Headlines From Around the World — and Why They Matter to You

The past year has seen several high-profile attacks:

	Production paused in all global plants due to a major attack.
	Serious disruption to website and retail operations.
	16.6 million customer records exposed.
	Hospital systems disrupted nationwide.
	Confidential health data stolen.
	An update failure caused billions in losses across sectors.
	Ransomware disrupted trading in the US Treasury market.

The clear pattern: attackers increasingly enter through a supplier or a software platform rather than the business itself. The Financial Times reports that 30% of all attacks now start through a third-party, double the previous year. This means your business can be hit even if you are not directly targeted.

3. Why SMEs Need to Act Now



Financial stress

A week-long outage from ransomware can be enough to put an SME into crisis.



Regulatory trouble

Losing personal data can lead to investigations, fines and mandatory reporting.



Losing customers

Large customers now expect suppliers to show that they have basic cyber protections in place. Failure to meet these expectations can lead to losing work.



Insurance challenges

Cyber insurers may refuse claims if the business wasn't following basic good practice. Cybersecurity is not just an IT problem — it is a matter of business continuity, cash flow, and customer trust.

4. The “Basic Six”: Simple Steps That Prevent Most Attacks

These six actions are low-cost and easy to put in place. They stop the majority of cyber incidents:



1. Turn on Multi-Factor Authentication (MFA) — especially for email and finance systems.



2. Back up your data and test that you can restore it.



3. Keep software and devices updated automatically.



4. Use a password manager and avoid password reuse.



5. Train staff regularly to spot suspicious emails and messages.



6. Limit who has admin access to your systems.

If you want to go further then consider:

- 7. Inventory & asset management:** Know all the systems, devices, and applications you run. See what you've got before you can secure it.
- 8. Network segmentation / least-privilege access for systems:** Ensuring that if one system is compromised it doesn't give full access to everything.
- 9. Endpoint detection and response (EDR) and monitoring:** Active monitoring and detection of anomalies.
- 10. Incident response planning & testing:** Having a plan for what happens if you are attacked (and rehearsing it) is often overlooked by SMEs.
- 11. Supply-chain / vendor risk management:** Check the security of their external suppliers and technology providers.
- 12. Secure configuration / removing unnecessary services:** Ensure default settings are locked down, unused services disabled, etc.
- 13. Regular testing & drills (phishing simulations, restore tests, firewall reviews):** Ongoing verification is important — controls must be maintained and tested.

5. AI: The New Risk — and the New Defence

How attackers use AI

- Creating fake emails and messages that look real
- Spotting weak points in systems faster
- Running more convincing invoicing and payment scams
- Automating password-guessing

How businesses use AI

- Spotting unusual behaviour instantly
- Speeding up security fixes
- Guiding teams during an incident
- Providing clearer risk insights

IBM warns that companies using AI without proper checks and controls are more likely to face a serious breach. AI helps — but only when used responsibly.



6. Leading Through a Cyber Crisis

Cyber incidents don't behave like ordinary business problems. Leaders should prepare for three key moments:

1. **Disruption:** What happens if key systems suddenly stop working?
2. **Ransom decisions:** Agree your principles before you are under pressure.
3. **Notifying customers:** Plan how to communicate clearly and calmly about data loss.

Every organisation should set up alternative communication channels, test its response plan twice a year, and make sure everyone knows their role. Developing trust and using clear communication before, during and after an incident are essential.

7. Key Actions for Business Leaders in 2025

Treat **Cybersecurity** as a **top-level business risk**.

Review your **entire supply chain**, not just your own systems.

Make sure your business has **basic protections** in place.

Strengthen **cash flow plans** — SMEs are more vulnerable.

Test your incident plan at least twice a year.

Use **AI carefully**, with **proper oversight**.

Cyber resilience is achievable for every organisation — and in 2025, it is essential.

Conclusion

Cyber threats are growing quickly, but the steps to defend against them are clear and manageable. By putting the basics in place, checking supply chain risks, and preparing for how you will respond, your organisation will be far more resilient.

Cybersecurity has become a fundamental requirement of modern business. The decisions you make today will determine how well your organisation survives tomorrow.



Appendix 1 - Sources & Further Information

For organisations wishing to deepen their understanding or benchmark their own preparedness, the following credible sources provide authoritative insights:

Government & Public Sector Sources

- UK Government Cybersecurity Breaches Survey 2025 – statistics on business cyber incidents, costs and vulnerabilities
- National Cybersecurity Centre (NCSC) – “10 Steps to Cybersecurity” and practical SME guidance
- European Union Agency for Cybersecurity (ENISA) – annual threat landscape reports

Industry & Technology Research

- Microsoft Digital Defense Report – analysis of global threat actor activity
- IBM Security X-Force Threat Intelligence Index – trends in ransomware and AI-enabled attacks
- Financial Times Cyber Reports – data on supply chain attacks and enterprise risk

Regulatory & Compliance

- Information Commissioner’s Office (ICO) – guidance on GDPR, reporting duties and breach penalties
- U.S. Securities & Exchange Commission (SEC) cyber rules – expectations for large organisations and financial-sector preparedness

Further AGN Reading

- AGN Digital Maturity Diagnostic Tool – including cyber and data security maturity dimensions.
- The AGN Advisory Migration Methodology – moving from compliance to advisory (with cyber as a natural advisory vector).
- AGN Membership Global Outsourcing Survey – opportunities for member-to-member and partner-based outsourcing, including cyber.



Contact:

For further information on this topic or anything relating to the AGN International association of accounting and advisory firms, or to become an AGN member, please email your closest AGN Regional Director (see below) or go direct to www.agn.org.

Malcolm Ward
CEO AGN International
mward@agn.org

Robert Zhang
APAC Regional Manager
asia-pacific@agn.org

Marlijn Lawson
EMEA Regional Director
mlawson@agn.org

Cindy Frey CPA, CGMA
Americas Regional Director
cfrey@agn.org

excellent.
connected.
individual.



For further information, or become involved, please contact:

AGN International

Email: info@agn.org | Office: +44 (0)20 7971 7373 | Web: www.agn.org

AGN International Ltd is a company limited by guarantee registered in England & Wales, number 3132548, registered office: 3 More London Riverside, London, SE1 2RE United Kingdom. AGN International Ltd (and its regional affiliates; together "AGN") is a not-for-profit worldwide membership association of separate and independent accounting and advisory businesses. AGN does not provide services to the clients of its members, which are provided by Members alone. AGN and its Members are not in partnership together, they are neither agents of nor obligate one another, and they are not responsible or liable for each other's services, actions or inactions.

Copyright © 2025 AGN International Ltd.