SEPTEMBER 2025

CURATED

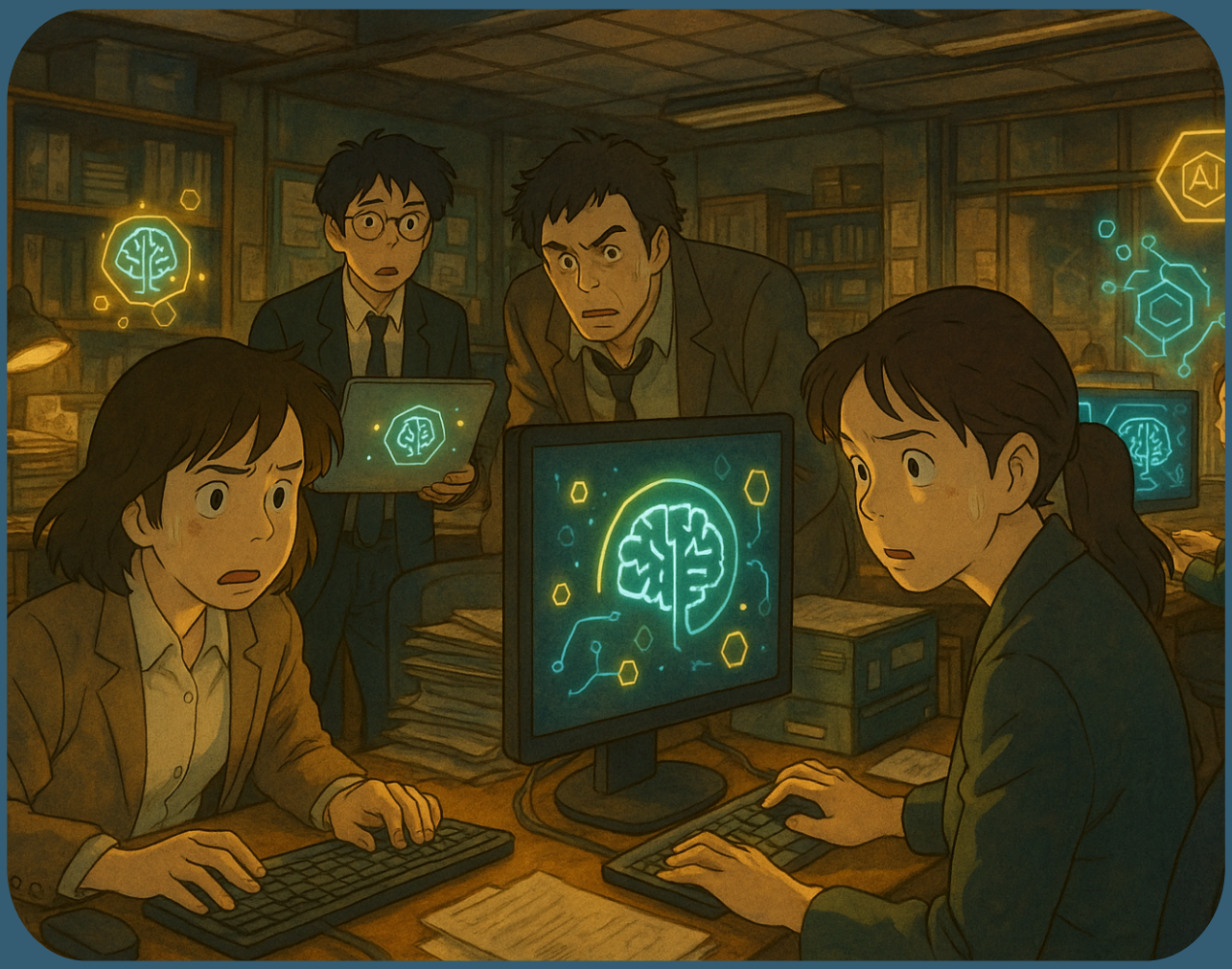
SO WHAT?

EFFECTIVE INCIDENT RESPONSE IN THE ERA OF AI AND NEW CYBER REGULATIONS

READ ON

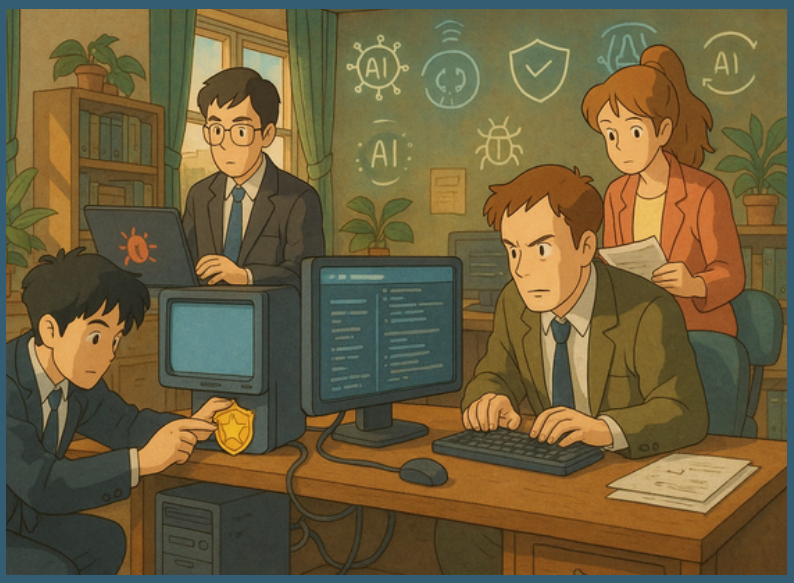
Introduction

In 2025, cyber threats are changing fast. Artificial Intelligence (AI) is now being used by bad actors to launch more advanced and convincing attacks. At the same time, new laws like the UK Cyber Security and Resilience Bill require businesses to act quickly and transparently when a cyber incident occurs. This makes having an effective incident response plan essential for every business, big or small.



What is an Incident Response?

Incident response is the process your business follows when it detects a cybersecurity problem, such as a data breach, ransomware, or phishing attack . It involves:



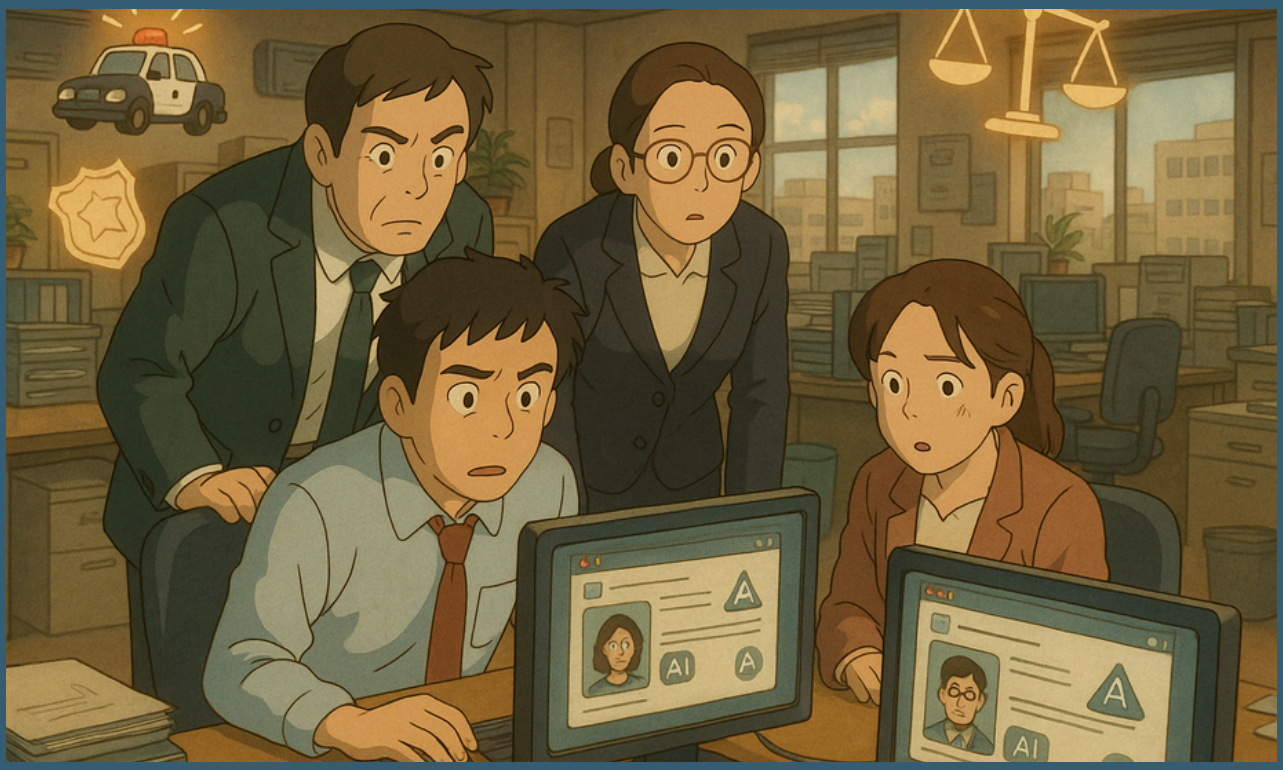
- **Quickly identifying the issue.** This means detecting as early as possible when something unusual happens in your network or systems, whether it's a hacking attempt, malware infection, or unauthorised access.
- **Containing the threat to stop it from spreading.** Once the problem is identified, taking immediate action to stop it from spreading or causing further damage. This could involve isolating affected systems or blocking malicious traffic.
- **Removing the attack or fixing the vulnerability.** Cleaning up after the incident by removing malware, closing security gaps, and patching software or hardware weaknesses that were exploited.
- **Recovering systems back to normal operation.** Restoring systems and data to their proper working condition, which may include rebuilding systems, restoring data from backups, and validating that everything is secure.
- **Reporting the incident as required by law.** Many regulations require businesses to report certain types of cyber incidents to authorities within a specific time frame. Proper documentation and timely reporting ensure compliance and help limit legal consequences.

With AI-powered attacks growing more sophisticated such as fake emails mimicking trusted contacts or deepfake audio/video hacks these steps must happen faster and with greater precision to reduce risk and damage.

In summary, incident response is your business’s safety plan for handling cyber emergencies quickly, effectively, and in line with legal requirements, helping you protect your data, systems, and reputation.

Why AI Makes Incident Response More Urgent

Hackers now use AI to create fake emails that look just like messages from colleagues or suppliers, fooling many people. They can also use “deepfakes”, fake videos or audio, of real people in businesses, so that colleagues are fooled into transferring money or sharing sensitive data. These AI tools speed up attacks and make them harder to spot, so your incident response plan needs to be ready to deal with these new tricks.



Understanding New Cyber Regulations

The new Cyber Security and Resilience Bill requires businesses to:

- Report cyber incidents within 24 hours of discovery
- Show clear evidence of the security measures they have in place
- Prove they have tested their response plans regularly

Benefits of Having an Effective Incident Response

- Early Detection: Tools powered by AI can monitor your systems and alert you quickly about unusual activity.
- Clear Procedures: Knowing exactly what to do and who to contact saves valuable time during a crisis.
- Compliance Assurance: Being prepared helps you meet legal requirements and avoid penalties.

- Minimised Damage: Acting fast limits data loss and downtime, reducing financial and reputational harm.
- Improved Confidence: Customers and partners trust businesses that show they can handle problems effectively.

Steps to Build Your Incident Response Plan

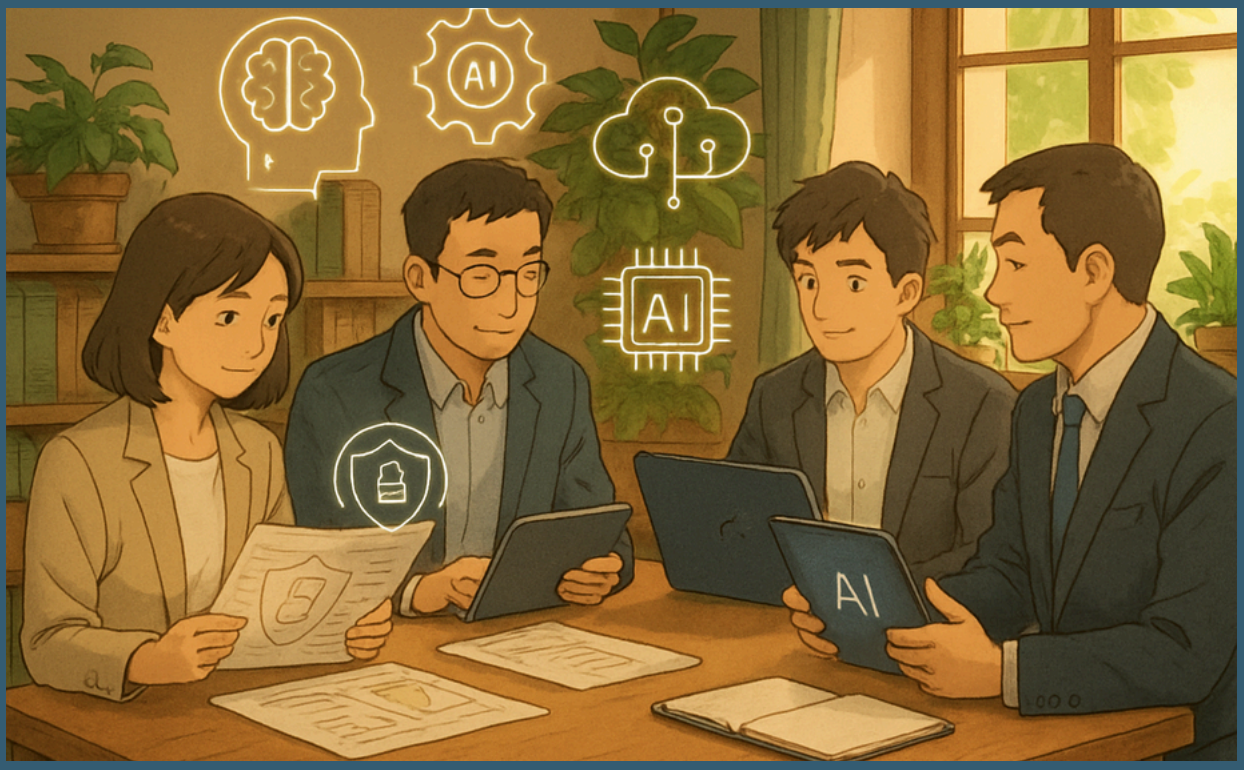
- Assign Roles: Decide who leads the response, who communicates with stakeholders, and who fixes the technical issues.
- Create Clear Procedures: Write down the steps to identify, contain, and fix incidents.
- Train Staff: Regularly train employees on cybersecurity basics and how to recognise suspicious signs.
- Test the Plan: Practice with simulated attacks to find gaps and improve your response.
- Use Technology: Employ AI-driven monitoring tools to catch threats early.
- Document Everything: Keep records of incidents and responses to support compliance and future improvements.
- Prepare for Reporting: Know who will notify regulators and what information is required.

Final Thought

Today, incident response is no longer just an IT issue, it's a business priority. AI-driven cyber threats and stricter laws mean you must be ready to act fast, stay compliant, and protect your business reputation. The good news is that with a clear plan and simple steps, any business can strengthen its defences and respond effectively.

Start today by reviewing your current capabilities. A strong incident response plan will help you stay resilient in a world where cyber risks are growing by the day.

Stay safe, stay prepared, and keep your business running smoothly.



If you dont have an Incident Response Plan, or have an old one and want to update it, or to talk to us more about how you might implement any and all of the above:

email: enquiries@incommsec.com

Jump on a quick call: https://calendly.com/mike-q/cyber-security

We look forward to talking with you.

SEPTEMBER 2025

CURATED

WANT TO HAVE A SAY?

ASK A QUESTION OR GET IN TOUCH

ENUIRIES@INCOMMSEC.COM