Incident Readiness – What Happens If Something Goes Wrong?

This one pager is designed to help organisations understand whether they are practically ready to respond to a cyber incident. It is not a technical guide however it is a good starting point towards building a strong cybersecurity plan.

Ownership and authority

Do you know who is responsible for declaring a cyber incident?

- Who decides that an incident is happening
- Who has authority to make decisions during the incident
- Who signs off communication to customers, regulators, or partners

If responsibility is assumed rather than clearly assigned, response will be delayed.

First actions

In the first hour of a cyber incident, do people know what to do?

- Who is contacted first
- What systems or accounts should not be touched
- How evidence is preserved
- What information should be recorded immediately

Panic and well intentioned actions often make incidents worse.

www.sccyber.co.uk
info@sccyber.co.uk

Internal escalation

Once an incident is identified, who needs to know?

- IT or security leads
- Senior management
- Legal, compliance, or risk owners

Uncontrolled email chains and informal messaging create confusion and gaps.

External contacts

Do you know who to contact outside your organisation?

- IT or security suppliers
- Incident response partners
- Cyber insurance contacts
- Legal advisors

Contact details should be known in advance, not searched for during an incident.

Third party involvement

If IT or security is outsourced, who manages the supplier during an incident?

- Who contacts the supplier
- Who challenges and validates their response
- Who decides whether external advice is required

Responsibility cannot be fully delegated, even when services are outsourced.

www.sccyber.co.uk
info@sccyber.co.uk

Regulatory and reporting considerations

Do you know if the incident needs to be reported?

This may involve regulators, customers, partners, or insurers.

You do not need to know the exact thresholds, but you should know who assesses them.

After the incident

Once the immediate issue is contained, what happens next?

- Documenting what happened
- Understanding root causes
- Reviewing supplier performance
- Identifying lessons learned

Without this step, the same incident is likely to happen again.

Why this matters

Many organisations believe they are prepared for a cyber incident. In practice, preparation often exists only in contracts or assumptions.

If you cannot confidently answer the questions above, there is a gap between expectation and readiness and you should contact SCCYBER for help as soon as possible.

www.sccyber.co.uk
info@sccyber.co.uk