Importance of having a plan in place

Minimizing the Impact of Cyber and Data breach Incidents: a well-structured incident response plan enables organizations to act quickly and efficiently when faced with a cyber threat.

An Incident Response plan is a written plan, with clearly defined set of procedures designed to recover operations and minimize downtime, protect its clients and customers and its own reputation, minimize financial losses and protect share price.
Without a formal IR plan in place, organizations may not detect attacks nor know what to do to contain, clean up and even prevent the ever increasing threat of attacks.

Development of an Incident Response Plan

The TrustBridge's Incident Response Plan: comprehensive and implementable

Our Incident Response Plans include:

- Data Breach and Cyber Incident policy and processes
- Method of Identification of Incident / Breach detection and analysis
- Internal Incident Report Structure and template
- Incident Escalation Process to include clear definition of
  - contact points, escalation, communication
  - decisions that need to be made quickly and under pressure
  - the legal requirements
  - Insurance company involvement
- Incident Response Flowchart and Procedure
- A checklist for evidence for risk assessment and decision making
- Identification and structure of Incident Response Team – roles and responsibilities
- Incident Management process
  - Containment
  - Eradication
  - Recovery
  - Notification
- Communication requirements
  - Notification to regulatory authorities
  - To Personal Data Subjects
  - To employees and partners
  - Media and Social Media
- Business Continuity plan and critical systems structure

The Incident Response Plan can be supported by training for all employees:

- Crisis Simulation Scenario based Workshop: a face to face bespoke simulation which includes:
- Online training course (circa 3 hours) accredited by the UK Government's National Cyber Security Centre.
- A full briefing of all the leadership team / stakeholders and the key employees to ensure that everyone understands how to implement, and the key decisions and actions that need to be undertaken, in an emergency situation and whilst under pressure.

The Trust Bridge Approach

Outcome

- **Preparedness:**
  Adequate preparation will help in rapid decision-making.
- **Efficient Detection:**
  Quick identification of security events, reducing response time.
- **Containment and Recovery:**
  Swift actions to contain and eradicate the issue, reducing potential damage.
- **Compliance:**
  Adherence to industry standards like NIST or ISO 27001, and data protection regulations which could be mandatory for some businesses.
- **Learning and Adaptation:**
  Post-incident analysis will guide future strategies and preparations.
- **Leverage of Resource:**
  Ensure staff and resources are maximised.

Certainty

The TrustBridge's due diligence provides a high level of certainty when assessing data protection and cyber security practices.

- **Predictability:**
  Enhanced foresight into how incidents are managed.
- **Time-Saving:**
  Faster response and resolution times.
- **Financial Benefits:**
  Reduced costs from minimizing impact.
- **Compliance Certainty:**
  High likelihood of meeting regulatory standards.
- **Strategic Confidence:**
  Insights for future planning.
- **Confidence Level:**
  High

www.thetrustbridge.co.uk

Contact us

Phone: US: 803 348 0000 or UK +44 7768 962 480
penny.heyes@thetrustbridge.com or alan@thetrustbridge.co

No.	Item	Description	Option 1	Option 2	Option 3
1	Incident Identification	Ability to quickly identify and categorize security incidents based on their severity and potential impact.	✓	✓	✓
2	Incident Response Team Formation/Review	Establishing a dedicated team with clear roles and responsibilities to handle incidents.	✗	✗	✓
3	Communication Protocols	Clear guidelines on internal and external communication during and after an incident, including stakeholder notification.	✗	✓	✓
4	Incident Analysis	Tools and procedures to analyze the root cause, extent, and impact of the incident.	✓	✓	✓
5	Containment Strategies	Short-term and long-term measures to contain the incident and prevent further damage.	✗	✓	✓
6	Recovery & Restoration	Steps to restore affected systems and services to their normal state.	✗	✗	✓
7	Post-Incident Review	A structured review process to learn from the incident and improve future response.	✗	✗	✓
8	Training & Awareness	Training sessions for employees and stakeholders on incident response and cybersecurity best practices.	Online Course	Online Course	Workshops
9	Legal & Regulatory Compliance	Ensuring the incident response plan aligns with UK regulations and legal requirements, including GDPR.	✓	✓	✓
10	Third-party Coordination	Protocols for coordinating with third-party vendors, partners, and law enforcement during an incident.	✗	✗	✓
11	Incident Simulation & Drills	Testing the incident response plan through simulation and drill to ensure effectiveness.	✓	✓	✓
12	Bespoke Cyber Simulation	Technical / Legal / Reputational / Communication Identification of incident: triggering the incident response plan Escalation Steps to take Evidence and documentation of decisions Communication: media / social media Shaping a legally defensible narrative Control the Messaging (internally and externally)	✗	✗	✓
13	Documentation & Record Keeping	Template for detailed records of all incidents, responses, and lessons learned for future reference and compliance.	✗	✗	✓
14	Stakeholder Management	Managing relationships with stakeholders, including customers, investors, and regulators during and after an incident.	✓	✓	✓
	Total GBP£	**Circa**	**£4,750**	**£9,550**	**£29,750**

Component	Difficulty in Implementation	Estimated Value
Incident Identification	Medium	High
Incident Response Team Formation/Review	Medium	High
Communication Protocols	Low	High
Incident Analysis	High	Very High
Containment Strategies	High	Very High
Recovery & Restoration	High	Very High
Post-Incident Review	Medium	High
Training & Awareness	Low	High
Legal & Regulatory Compliance	Medium	High
Third-party Coordination	Medium	High
Incident Simulation & Drills	Medium	High

www.thetrustbridge.co.uk

TTB are co owners of an UK GDPR certification scheme with the UK regulator (ICO) approved certification criteria