Data Breach Response Plan Checklist

Businesses must protect the privacy and security of the personal data and confidential information in their custody and control. However, in today's dynamic threat environment, businesses are facing evolving risks to their information technology (IT) systems and networks. To mitigate these risks, a business should build a data protection program tailored to its unique concerns and threats. **Central to developing a data protection program is creating, implementing, and maintaining a clear and concise data incident response plan (IRP) that outlines the measures and tools needed to prepare for and respond to an actual or reasonably suspected data breach**. This checklist provides an outline of the critical elements a business should address or consider when creating an IRP**.**

✔ **Purpose, scope, and key terms.** The IRP must address the business's unique structure, personnel, and available resources, including when and where the IRP applies.

- ☐ A business's employees, contractors, and agents may have varying levels of access to data, and the IRP should address each, based on likelihood of risk and potential harm.

✔ **Governance and responsibilities** The IRP must identify the key individuals who have roles in the security incident response process. It should include an appendix containing the individuals' names and contact details, including any secondary members, and should identify:

- ☐ The executive management team composed of the most senior personnel responsible for overseeing a data security incident.
- ☐ In-house and external counsel responsible for legal advice on data security incidents and all matters pertaining to information security.
- ☐ The officials responsible for human resources, including those knowledgeable about the business's benefits programs (e.g., health and wellness, retirement).
- ☐ The subject matter experts on the business's IT infrastructure and environment.

✔ **Incident Response Coordinator**. The business should delegate authority to one person, an Incident Response Coordinator, to oversee data breach response efforts, including authority to:

- ☐ Implement, maintain, and update the IRP.
- ☐ Assemble an Incident Response Team (IRT) and coordinate incident response activities.
- ☐ Conduct post-security incident reviews.
- ☐ Provide training and conduct exercises.

Is it a data breach or a security incident?

The term "data breach" generally refers to the unauthorized use, processing, or disclosure of, or access to, personal data in the custody or control of a business. It is often used in the legal context to convey a business's regulatory or contractual obligations to notify individuals, government agencies, and other third parties of the incident and to undertake certain remedial measures. The term "security incident" often refers to an unanticipated or prohibited event or anomaly within an IT environment or the impermissible processing of personal data, which could be caused by an external threat actor, malicious insider, or human error. A business must promptly respond to a security incident to assess whether it has resulted in a data breach.

✔ **Incident Response Team.** An IRT is a predetermined group of employees, contractors, and other resources responsible for responding to data security incidents. An IRT must:

- ☐ Provide a timely, informed, and effective response to security incidents to avoid loss or damage and minimize economic, reputational, or other harm arising from security incidents.
- ☐ Prioritize incident response over other work responsibilities.
- ☐ Include team members with experience in different areas, with a special emphasis on IT, legal, HR, communications, compliance, and consumer relations.
- ☐ Identify external resources, including forensic service providers and IT consultants, outside counsel, and applicable cyber insurance providers.

Data Breach Response Plan Checklist

✔ **Incident response procedures.** The IRP should include procedures and protocols that address each of the following:

- ☐ ***Detection and discovery***. Technical security controls that generate automated security incident alerts and provide other means for employees and third parties to report security incidents or vulnerabilities (e.g., internal breach response email address, external vulnerability disclosure program).
- ☐ ***Assessment and escalation***. A process to assess a security incident to identify whether there is a potential data breach and, based on the assessment, activate the IRT.
- ☐ ***IRT investigation and analysis***. On activation, the IRT should investigate each data security incident, including evaluating systems linked to the incident, identifying whether data was exfiltrated from the business, determining whether the incident involved ransomware, and identifying whether the data security incident originated from a customer or vendor.
- ☐ ***Containment, remediation, and recovery***. The IRT should execute a plan to contain, remediate, and recover from each identified security incident, which may include disabling or segregating affected IT systems; identifying backup and other redundant sources of the affected data and managing data restoration; retrieving, to the extent permitted by law, data that was lost, stolen, or compromised; determining whether connection with third-party systems exposes the business to vulnerabilities; and disabling access to the IT network or systems.

✔ **Evidence preservation**. The IRT should direct appropriate internal or external resources to capture and preserve evidence during the investigation, analysis, and response activities by:

- ☐ Securing access to IT systems, networks, and devices to maintain their integrity.
- ☐ Retaining access logs and surveillance videos.
- ☐ Executing chain of custody documentation.
- ☐ Refraining from using legal and technical terms (e.g., personal data breach) in internal records unless necessary.

✔ **Communications and notifications**. The IRT, in coordination and consultation with legal counsel, should consider developing a communication plan for both internal and external stakeholders, which should address:

- ☐ Whether the business is legally required to issue reports or notifications to individuals whose personal data may have been compromised, law enforcement or government authorities, or other third parties (e.g., insurance companies, banks, or credit agencies).
- ☐ Whether there are any content requirements for external communications.

Breach Notification Letters

Most data breach notification laws require a business to provide notice of a data breach in a timely manner so individuals impacted by the breach can undertake measures to mitigate potential harm (*e.g.,* change usernames and passwords, monitor financial accounts). In addition, many of these laws require these data breach notices to include certain content about the incident. A business should consider identifying any applicable content requirements and including a draft data breach notification letter as an appendix to the IRP to streamline the notification

✔ **Post-incident response.** Following a security incident or data breach, a business should, at least periodically, reconvene the IRT to assess the incident, the effectiveness of the response, and any remedial measures needed to mitigate risk. The assessment should address:

- ☐ The nature and volume of data compromised, and the parties and systems involved in the incident.
- ☐ How the incident evaded security controls, and whether the incident could have been prevented through existing processes.
- ☐ The steps taken to investigate, contain, and mitigate the incident, and how well staff (including the IRT) performed.
- ☐ Whether the IRP's procedures were followed during the incident response and whether any deviations thereto were authorized.
- ☐ Any relevant recommendations.

If your organization has suffered a data breach or incident, please contact us at any time (24/7) and a Thompson Hine cybersecurity attorney will respond to you as soon as possible.
Contact us at: ThompsonHine.com/services/privacy-and-cybersecurity/contact