Data Breach Avoidance and Response Plan Checklist

by *Elizabeth A. Rogers*, Michael Best & Friedrich LLP

In order to minimize data breach risk and address a data breach promptly and effectively, your clients should prepare plans for both avoidance of the breach and how to respond in the event of a breach. These checklists provide guidance on what should be included in such plans. For a more detailed discussion on preparing data breach avoidance and response plans, see *Data Breach Planning and Management*.

Creating a Data Breach Avoidance Plan

In order to minimize risk, a business should adopt a data breach avoidance plan before a breach occurs. As part of a comprehensive data breach avoidance plan, a business should:

1 Create a data map of all the data collected by the business. The data map should contain detailed information about each piece of data, including:

- The type of data
- From whom the data is collected (and why)
- How the data is collected and input
- How and where the data is stored
- Who can access the data, and how (and where those persons are located)
- The purposes for which the data is used
- Whether and how the data may be altered or manipulated, by whom, and for what purpose
- Whether and how the data may be transmitted
- How the data is secured
- How long the data is retained
- How the data is disposed of or destroyed
- Any backups to the data
- Logs or documentation pertaining to the data

2 Assess and document the laws, regulations, and industry standards that apply to each piece of data (and make sure there are policies and procedures in place to ensure compliance).

3 Categorize the data based on its sensitivity and the severity of the legal impact to the business in the event of a breach (e.g., regulated, confidential, or sensitive data; internal or private data; public data).

4 Implement appropriate administrative, electronic, and physical data security safeguards (along with corresponding written policies and procedures). Data protection and management measures may include:

- Encryption of data and other security measures such as firewalls, network segmentation, and strict password requirements
- Monitoring systems (e.g., telephone and email/Internet use monitoring, video surveillance systems)
- A Bring Your Own Device (BYOD) policy that addresses whether, and under what circumstances, employees may use their own devices (such as laptops, iPads, smartphones, or other mobile devices) for work purposes
- A records retention/destruction policy
- Employee training manuals and programs that specifically address data protection measures, and identifying and reporting breaches, pursuant to the business's internal policies and procedures

5 Adhere to data security and privacy representations that appear in privacy policies or other public and/or consumer-facing statements.

6 Assess existing relationships with third party vendors, conduct due diligence of potential vendors' data security and privacy practices, and include appropriate protections in any contractual agreement. Key contractual terms might include:

- Data protection requirements
- Notification requirements in the event of an actual or suspected breach
- Indemnity provisions or other exclusions or limitations of liability
- The right to access or audit the third party's security measures onsite (or, alternatively, the third party is required to conduct and submit an annual security assessment)

7 Consider purchasing cyber insurance.

Creating a Data Breach Response Plan

In addition to a data breach avoidance plan, as part of best practices, a business should also create a data breach response plan that thoroughly details how the business will respond to a data breach and the requisite timelines. As part of a comprehensive data breach response plan, a business should:

1 Assemble a data breach response team, making sure to clearly define the roles and responsibilities of each team member. Team members should include:

- An incident lead (such as the business's Chief Information Security Officer)
- Information technology (IT) representatives
- Data privacy representatives
- Legal and risk management representatives
- Public relations/affairs/communications representatives

- Human resources (HR) representatives
- Customer service representatives

2 Outline the steps that each team member should take following the report of a data breach (and when), including the following critical actions:

- Securing the data and systems to stop the breach
- Identifying the scope of the breach, the compromised data, and the affected individuals
- Determining which state and/or federal laws are applicable
- Notifying the affected individuals
- Managing communications as to the data breach and the steps taken to investigate and respond to the breach

3 Compile a list of outside vendors and agencies that may need to be consulted or notified in the event of a breach, such as:

- Computer forensics experts
- Outside counsel
- Call center services
- Fraud or credit monitoring services
- Credit restoration services
- Law enforcement and government agencies

4 Test the response plan on a regular basis and make adjustments as necessary.

5 Assess and document, post-breach, the effectiveness of the response plan and any mitigation efforts.

End of Document