Data Breach Incident Response Plan
Best Practices

David J. Oberly

Today, the list of corporate cyber attack victims grows more numerous every day. To complicate matters even further, cyber criminals continue to become ever-more sophisticated in their skills and attack methods as time progresses. In 2019, the question is not a matter of *if* your organization will experience a data breach, but rather *when* and *how* a breach will take place. While many organizations have taken significant measures to prevent data breaches, the majority of business entities operating today have failed to properly prepare themselves with the tools and resources to effectively manage the data breach response process. With the average cost of a data breach having risen to a staggering $3.86 *million* per incident, those entities that fail to properly prepare themselves to effectively manage major security incidents do so at extreme peril. Fortunately, by utilizing the data breach incident response plan best practices discussed in this article, organizations—including law firms—can properly prepare themselves to minimize the impact of a data breach event when that inevitable time comes.

Data Breach Incident Response Plan Elements

Effective incident response plans provide a framework for taking action after a breach, where vital decisions are made ahead of time and, as such, do not have to be made on the fly and under pressure. There are a myriad of variations, but the best incident response plans typically encompass the following elements, which should be used as a template and then tailored to meet the unique needs of each individual organization.

The Incident Response Team

First, incident response plans need to identify the members of the business's incident response team—the key players who will be involved in the breach response process—and the roles they will play in reacting to a breach event. Once a breach occurs, there will be a multitude of responsibilities that need to be fulfilled, and the response plan should delineate and detail exactly who will step in to fulfill these roles. Importantly, incident response teams must combine both internal and external resources who can be mobilized immediately after a breach occurs. In this respect, the plan should first identify all internal team members, including members of the organization's IT, privacy/compliance, customer service, legal, and communications departments. In addition, the plan should also include information on key outside contacts, such as forensics investigators, identity theft vendors, breach notification vendors, insurance providers, public relations/crisis management firms, and outside counsel, all of whom will likely be needed to properly respond to a data breach.

Containment and Eradication

Next, incident response plans must include policies, procedures, and practices for containing and eradicating a security incident once a breach has taken place. Here, response plans need to provide detailed guidance as to how team members can take action to reduce and mitigate

the impact of the breach to the greatest extent possible, and to keep the breach from spreading and causing additional damage to the company. In particular, the plan should provide organizations on how to identify and secure all impacted data, devices, and systems, as well as how to isolate and preserve the compromised data. All accounts that have been compromised must be isolated and disabled. If the breach encompasses any form of virus or malicious code, the proper recourses should be mobilized to clear these hazards from the organization's networks and systems. In addition, all organizational passwords and encryption keys should be immediately changed once a breach is detected, as it is likely that an attacker will try to breach the entity's systems more than once.

Communication

Many incident response plans address the technical side of responding to a breach, but it is equally as essential that each phase of the incident response plan addresses communication as well, as the quality of the breach response team's communications in the wake of a breach event can play a significant role in minimizing the financial and operational fallout of a breach. There are two primary aspects to communication that must be addressed in the plan. First, the plan should detail the organization's internal communication procedures and responsibilities following a breach.

Second, the plan should also provide guidance on all external communications that may become necessary following a breach. In particular, the plan should provide contact information and guidelines for consulting with legal counsel. It is essential that breach victims get sound legal advice as early as possible so that they can avoid the severe adverse legal consequences that flow from improperly responding to a data breach, most particularly class action lawsuits that often arise in the wake of security incidents. In addition, the utilization of an outside public affairs or crisis management team may be necessary in order to ensure that the business's data breach notifications are phrased a strategic, yet straightforward, manner. Finally, the plan should provide a strategy for notifying customers if their information is improperly accessed, which should be done as soon as possible, and within the mandated timeframe of federal, state, and local laws.

Remediation & Recovery

Incident response plans must also include measures that will be taken to remediate and recover from a data breach event by removing the threat and restoring impacted systems to their pre-beach capacity, ideally while minimizing data loss. This aspect of the incident response plan should provide a roadmap as to how breach threats will be removed, and a process for verifying that systems are not still compromised when they are brought back into operation. In addition, this part of the plan should also discuss how the company will timely restore any operations or services that were adversely impacted by the breach to minimize the financial consequences of the breach event. Moreover, as part of the remediation process, the entity may also wish to mobilize a public relations response team. Finally, the plan should include a summary of the key data privacy regulatory requirements for each jurisdiction in which the organization operates, so that it can comply with all legal requirements that come with experiencing a data breach.

Post-Event Analysis

The final element of an effective incident response plan relates to post-event analysis, which should take place as soon as possible after a breach event, preferably within the days immediately following a breach. Post-breach evaluations are key to analyze what happened during the incident and assess how the organization's team handled mitigating the impact of the breach event. In addition, organizations should conduct a complete investigation of the cause of the breach, and consider any potential changes that need to be made to the company's policies and procedures in order to improve the company's cybersecurity defenses and its ability to thwart and minimize breach events in the future.

Incident Response Testing & Training

Importantly, merely implementing an incident response plan is only half the battle when it comes to effective data breach response. In addition, once an entity's response plan has been finalized and put into place, that plan needs to be tested often and under real-life conditions to ensure that the organization's employees are able to perform in an efficient and effective manner in the event the plan must be put into action. In particular, simulating data breaches and tabletop exercises are both effective ways of properly planning and preparing employees to perform to the level necessary when a breach incident takes place. In addition to preparing employees for the real thing, businesses can also use this training to modify their plans and make improvements in any weak points that are identified during these simulated events.

Conclusion

As the brazenness, frequency, and severity of data breach events continues to increase with no end in sight, now more than ever companies must be proactive in implementing robust data breach incident response plans to mitigate the risk posed by data security events. As such, an effective written data breach incident response plan should be a paramount focus of all businesses—including law firms—as a proper incident response plan can play a critical role in reducing the financial, operational, and reputational impact that a security breach can have, and can save organizations thousands, if not millions, of dollars that would otherwise be expended in recovery expenses and operational disruptions. Through implementation of the key incident response plan elements discussed above, businesses can create and implement effective data breach response plans to ensure that they are properly prepared to react to and minimize the fallout of a data breach incident.

David J. Oberly is an associate attorney in the Cincinnati Office of Blank Rome LLP, and is a member of the firm's Data Privacy/Cybersecurity practice group. David can be reached at doberly@blankrome.com.