ETHICO

DATA BREACHES AND CORPORATE RESPONSIBILITY: WHAT TO DO IN THE FIRST 48 HOURS

Having a robust incident response plan in place and taking quick action following a data breach is critical for protecting your employees, customers, and stakeholders. Companies should be prepared for a breach and understand applicable data privacy laws and contractual controls. Rapid response demonstrates you are working diligently on behalf of anyone impacted. Failing to report breaches can also result in significant fines from regulators.

HOUR 1

DETECT, REPORT AND ASSEMBLE RESPONSE TEAM

At the first sign of a potential breach, immediately investigate and confirm whether sensitive data has been compromised. Alert key internal stakeholders like IT security, legal counsel, and executives to assess the situation. Quickly assemble your incident response team, outlining their roles and responsibilities. Having a team already assigned with clear processes eliminates delays in reacting.

Designate an incident manager to coordinate efforts, a public relations lead to handle communications, and identify technical personnel capable of investigating the breach's nature and scope. Legal counsel can advise on compliance obligations. External forensics experts may also need to be tapped for support. The response team should establish mechanisms to involve specialists in areas like forensics, law, public relations, and insurance.

Create an incident report template to capture key details such as date, time, description, impacted systems, and actions taken. Thorough documentation is crucial for reporting requirements.

HOURS 2-4

CONTAIN THE BREACH

A top priority is isolating and shutting down the affected systems to halt further data loss. Determine the scope by identifying which specific data, servers, databases, etc. have been impacted. Preserve evidence but avoid permanently destroying compromised data, as it can aid forensic investigation.

Engage cybersecurity firms for forensic analysis to uncover root causes, determine the extent of the breach, and prevent additional damage. They can also determine if any internal staff were complicit. Have technical staff monitor other systems for anomalies in case the breach has spread.

Document all actions taken during containment to account for evidentiary chain of custody. Identify and secure physical locations related to the breach. Preserve and analyze data from intrusion detection systems. Efforts should focus on regaining control over compromised systems.

Evidence gathering should not impede the containment process. However, data that could reveal breach size and scope should be collected. Work with your legal team to ensure containment procedures won't limit future litigation options.

HOURS 12-24

BEGIN RECOVERY PROCESS

Provide regular updates to affected individuals on investigation progress and how you are continuing to protect their data. Cooperate fully with external investigations from regulators and law enforcement. Transparent communication is essential for rebuilding trust.

Update the incident response plan with lessons learned during the breach. Conduct response exercises to validate improvements. Keep senior leadership and the board apprised of response measures and outcomes.

Although containment, reporting and recovery processes are underway, this is not the time to relax. Expect increased scrutiny from regulators, shareholders and customers around your security posture. Focus intently on rebuilding lost trust and mitigating long-term business damage. The average total cost of a data breach now exceeds $4 million.

Consider offering identity protection services to affected individuals for at least 1 year following the incident. Develop a public outreach strategy to help users protect themselves from potential consequences of the breach.

Strengthen controls for collecting, storing, and securing sensitive data to reduce likelihood of recurrence. Provide additional staff training on secure data handling. Routinely test systems to uncover vulnerabilities, and implement encryption technologies to render data unusable if stolen.

Post-breach priorities should include understanding root causes, improving defenses, keeping stakeholders informed, and leveraging the lessons learned to enhance resiliency.

HOURS 24-48

KEEP MOMENTUM

Provide regular updates to affected individuals on investigation progress and how you are continuing to protect their data. Cooperate fully with external investigations from regulators and law enforcement. Transparent communication is essential for rebuilding trust.

Update the incident response plan with lessons learned during the breach. Conduct response exercises to validate improvements. Keep senior leadership and the board apprised of response measures and outcomes.

Although containment, reporting and recovery processes are underway, this is not the time to relax. Expect increased scrutiny from regulators, shareholders and customers around your security posture. Focus intently on rebuilding lost trust and mitigating long-term business damage. The average total cost of a data breach now exceeds $4 million.

Consider offering identity protection services to affected individuals for at least 1 year following the incident. Develop a public outreach strategy to help users protect themselves from potential consequences of the breach.

Strengthen controls for collecting, storing, and securing sensitive data to reduce likelihood of recurrence. Provide additional staff training on secure data handling. Routinely test systems to uncover vulnerabilities, and implement encryption technologies to render data unusable if stolen.

Post-breach priorities should include understanding root causes, improving defenses, keeping stakeholders informed, and leveraging the lessons learned to enhance resiliency.

CONCLUSION

Responding quickly and effectively in the first 48 hours following a breach can significantly reduce short and long-term impact on your organization. Have detailed response plans in place before an incident occurs. Move rapidly to protect individuals, contain damage and demonstrate accountability. While technology and policies are important, proper handling of the critical initial hours comes down to having the right people and plans ready to take action.

With preparation and diligence, your company can recover from a breach, meet legal and ethical responsibilities, reassure stakeholders, and emerge stronger and more resilient. By following information security best practices and putting robust incident response processes in place before disaster strikes, companies can limit the damage and protect what matters most.