SURVIVE CYBER
TOOLS TO SURVIVE A BUSINESS CYBER ATTACK

Data Security Breach Incident Response Outline

Learn more at www.survivecyber.com
Enroll in Minutes

Pre incident response planning	• **Identify incident response team.** Having a team (internal personnel and external vendors) established (and hopefully tested) can provide a more rapid and efficient response capability. • **Develop an incident response plan**. Decision-making can become muddled in the heat of a security breach. An incident response plan can help to manage the chaos and mitigate risk. • **Test incident response plan**. Where possible and affordable, organizations should test their incident response plan and capabilities. Weaknesses or problems should result in the revision of the plan where appropriate.
Discovery of data security breach	• **Internal discovery and escalation**. Upon discovery of the data security breach the breach should be notified to relevant internal stakeholders, including escalation of notice to appropriate personnel authorized and equipped to handle incident response. • **Review and implement incident response plan**. If applicable. • **Notice to internal legal**. For purposes of establishing attorney-client privilege and coordinating response.
Establish Attorney-Client Privilege	• **Establishment**. Attorney-client privilege should be established and formalized as soon as possible after being notified of a security breach (whether using internal or external counsel). • **Outside Vendors and Privilege**. Outside vendors such as forensic professionals should be brought within the privilege so that the breached organization may argue that its communications on legal issues are protected under privilege. Communications by outside vendors should be routed through legal counsel. • **Internal Personnel and Privilege**. Internal personnel working on the breach should route their communications concerning the breach through the legal counsel so that the breached organization may argue that its communications on legal issues are protected under privilege.

Investigate and contain	• **Investigate status of breach**. After discovery of a security breach, the breached organization should investigate whether the breach is ongoing, whether the breach agent (e.g the method, such as malicious code, used to perpetrate the breach or data loss) is still active and whether the vulnerability that allowed the breach is still present and exploitable. • **Contain and eliminate the breach**. The organization should seek to contain and eliminate the breach, the breach agents and vulnerabilities. • **Use of Specialized Vendors**. As specialized security, IT or forensic services may be needed to contain and eliminate a breach, the breached organization should consider use of qualified third party vendors to assist with its efforts.
Response Team Formation and Activation	• **Multi-disciplinary efforts**. Security breaches can impact many different parts of and interests within an organization, and therefore may require the input and involvement of many different internal stakeholders, including without limitation, senior management, legal, IT, security, privacy, public relations/marketing and risk management/insurance. • **Form Internal Incident Response Team**. The organization should identify and create an internal incident response team, including potentially, a senior business manager with authority to make business decisions, legal, IT, security, privacy, risk management and public relations. The composition of the incident response team may vary depending on how the organization is structured internally. • **External Incident Response Team**. It is often more efficient and less risky to retain experienced third parties to assist in incident response. The external incident response team would typically include a lawyer and forensic professional. In addition, the team may include credit monitoring vendors, call center vendors and mail fulfillment vendors. The external team will coordinate and guide the breached organization in order to efficiently and effectively handle response efforts.

Initial Investigation	The breached organization should investigate the circumstances of the breach to: • determine how the breach occurred, including breach agents and vulnerabilities at issue • identify the data or systems that were impacted • identify third parties that may have been impacted or harmed because of the breach (e.g. clients, customers, employees, etc.) • identify parties that may have been responsible for the breach (e.g. third party service providers, internal employees, etc.) • determine if personal information, trade secrets, IP or other sensitive information was compromised • determine how to permanently eliminate the breach agent or remediate the vulnerability or problem that allowed the security breach to occur • ascertain the need to preserve data and potential evidence that may be relevant to actual or potential litigation, including identifying, preserving and collecting such data
Breach Notice Law – Trigger Investigation Phase	If personal information is involved it is necessary to determine whether the security breach triggers any obligations under existing breach notice laws, including: • determining whether and to what extent the personal information of individuals may have actually or reasonably been accessed by an unauthorized person • identifying the individuals whose personal information may have been exposed by the breach, including state of residency • analyzing which breach notice laws may apply and develop legal positions as to whether breach notice laws are triggered • for breach notice laws that have a "harm threshold" before notice is required, ascertain whether relevant harm has been suffered or may reasonably occur • develop a strategy concerning the steps necessary to comply with breach notice laws, scope of notice and actions necessary to effectuate notice

Breach Notice Law – Compliance Phase	If notification obligations have been triggered under breach notice laws, the organization should take steps to comply with applicable breach notice laws, including potentially: • drafting notice letters to individuals impacted by the breach that are compliant with the applicable breach notice laws • if the breached organization is a service provider storing or processing personal information on behalf of another organization that is the owner/licensee of that information, provide legally compliant notice to the owner or licensee • physically preparing and sending notices to impacted individuals based on methods set forth in breach notice laws, which typically means mailing notice (but can also include notice via email, public notice, and other methods prescribed by breach notice laws) • providing notice to law enforcement or regulators if required under the applicable breach notice laws, and coordinating with these entities as appropriate
Customer Relations and PR Efforts	In some cases a security breach could impact the reputation of the organization and harm customer and employee relationships. As such the following steps should be considered: • offering to provide credit monitoring services to individuals whose personal information was or may have been exposed (offering credit monitoring potentially also cuts off damages arguments should litigation be filed) • setting up and staffing a call center to provide information about the security breach to impacted individuals • stablishing a website or other online communication portal to provide information about the security breach to impacted individuals • engaging public relations/marketing professionals to develop messaging and public relations strategies to prevent or mitigate potential damage to and organization's reputation
Pre-Claim Litigation Readiness Phase	For serious **privacy breaches** with a high likelihood of litigation or regulatory action, it may be appropriate for the **insured organization** to prepare for potential litigation, including without limitation: • identifying potential legal violations of statutory, contractual or common law due to the security breach • developing legal positions, arguments and defenses with respect to potential legal violations • identifying third parties that may be liable (in whole or part) for the security breach (for purposes of potential cross-claims or indemnification), including for example service providers, security assessors, software vendors, payment processors, etc. • identifying, preserving and collecting data that may be relevant for evidentiary/e-discovery purposes in a lawsuit or regulatory action.

Claim/Litigation Defense Phase	In the event a claim, demand, lawsuit or regulatory action arises out of a security breach the breached organization should engage in the defense and resolution of that matter, including: retaining outside counsel for defense purposes • analyzing allegations and legal theories put forth by claimants or regulators • identifying potential legal violations of statutory, contractual or common law due to the security breach • developing legal positions, arguments and defenses with respect to potential legal violations • continuing to identify, preserve and collect data that may be relevant for evidentiary/ediscovery purposes in a lawsuit or regulatory action electronic discovery • claim resolution: settlement, trial, mediation, arbitration • any other defense activities that are necessary and reasonable under the circumstances surrounding the claim, demand, lawsuit or regulatory action

1. A data security or security breaches have a general flow of activity that transpires when the breach occurs. The following describes the general flow of a breach and an organization's response to the breach. Note that the phases do not have clear cut starting/ending points and often overlap and may not occur in strict chronological order.