

DATA SECURITY INCIDENT RESPONSE CHECKLIST

Prepared by
Jena Valdetero
Greenberg Traurig LLP
for the
MLRC Data Privacy Law Committee

February 2024



Data Security Incident Response Checklist

The following checklist is intended to be used once an organization's information security team has declared an incident. It is intended as a general guide and should be tailored to each organization.

<input type="checkbox"/>	1. Activate the Incident Response Team (IRT). The IRT should include representatives from cross-functional departments within an organization, including Operations, Legal, Finance, HR, and Communications.
<input type="checkbox"/>	2. Identify an IRT Response Leader. The Response Leader is responsible for coordinating the activities of the IRT and ensuring completion of identified tasks.
<input type="checkbox"/>	3. Set up a plan for regular meetings of the IRT using an out-of-band communications channel until forensics can confirm there is no compromise of the company's email or communications solutions.
<input type="checkbox"/>	4. Limit what is memorialized in writing until legal counsel is engaged and consulted to just the facts known at the time. Avoid speculation about the incident and self-criticism about the organization's security measures.
<input type="checkbox"/>	5. Evaluate the need to retain outside vendors, which could include forensic investigators, outside legal counsel experienced in advising on data breaches, crisis communications public relations, threat actor negotiators and crypto wallet payors (in the case of extortion or ransomware). Consider whether the vendors are pre-approved or will be approved by the organization's cyber insurance carrier, if any.
<input type="checkbox"/>	6. If legal counsel is engaged, ensure they are taking an active role in leading the investigation and that the IRT is instructed on how to communicate properly to preserve the strongest arguments that communications and reports related to the incident should be protected from disclosure by attorney-client privilege and the work product doctrine.
<input type="checkbox"/>	7. Notify the cyber insurance carrier of a potential claim. Many carriers require pre-approval of statements of work and proposals from vendors. Where time permits, the carrier should be consulted.
<input type="checkbox"/>	8. Identify stakeholders who will need or expect to be notified of a significant cybersecurity incident or who are likely to find out about such an incident. Stakeholders could include employees, board members, customers, vendors, regulators, and the public, including the media.
<input type="checkbox"/>	9. Notify law enforcement. While law enforcement generally is limited in how they can assist organizations with an investigation, law enforcement may have helpful intelligence about the threat actor.
<input type="checkbox"/>	10. Outline a communications plan designed to address how each category of stakeholder will be notified and kept informed of an investigation. Prepare communications holding statements concerning the incident to ensure consistent messaging to all stakeholders.
<input type="checkbox"/>	11. Ensure business continuity plans are activated in the event an incident results in the disruption of the ability to engage in normal business functions, either because of a compromise of systems or because systems have been taken offline proactively to mitigate any potential risk.
<input type="checkbox"/>	12. Identify all legal obligations to notify third parties, including regulators, affected individuals, and third parties for whom you may have a contractual notice obligation. Note that certain jurisdictions and regulated industries have regulatory notification obligations as short as 36-72 hours.
<input type="checkbox"/>	13. If sensitive personal information is determined to have been subject to unauthorized activity, consider whether notification is required by law or advisable, and develop a plan for ensuring notification is made timely and in accordance with applicable law. Consider retaining vendors to mail letters to affected individuals and provide, where appropriate, credit monitoring and ID theft protection services.
<input type="checkbox"/>	14. At the direction of counsel, prepare an "after action" report summarizing a timeline of events and key facts and findings. This report will be helpful in responding to follow up inquiries from regulators.
<input type="checkbox"/>	15. Following an incident investigation, the IRT should engage in an interactive after-action meeting led by counsel (to preserve privilege) to discuss what went well, what could be improved, and whether changes to the incident response plan should be made.