



Incident Preparedness & Breach Response

Contemporary connected business practices and environments require individually crafted data security programs. However, even with appropriate security controls in place, the risk of a data security incident remains high. Companies therefore also need to have an effective incident response plan in place together with a well-functioning team that has practiced how it will handle an inevitable data incident to minimize the potential impact of such an incident on their operations and reputations.

Short-Term Actions

When a data incident occurs, we work in tandem with internal and external resources including impacted business units, IT professionals, forensic investigators, breach notice providers and public relations professionals to execute a prompt and comprehensive response that accounts for both the legal and the security aspects of the incident. We work with the security team to protect the integrity and continuity of the potentially impacted system.

Because discovering how a data incident occurred is of vital importance, the forensic investigation effort is crucial. We are skilled in how to structure and direct investigations to optimize our clients' ability to assert privilege surrounding the investigation in the event of a litigation threat. We assess whether obligations to notify consumers, regulators or law enforcement have been triggered under applicable laws and regulations and work with our clients and breach notice providers to satisfy those requirements. We also advise on and assist with internal communications to boards of directors and the C-suite, as well as communications to employees, customers, individuals potentially impacted by the incident, law enforcement and regulators using strategies to avoid litigation and minimize possible penalties.

KEY CONTACT

David A. Wheeler
Incident Preparedness & Breach
Response

dwheeler@nge.com
D. (312) 269-5328

RELATED CLIENT SERVICES

Intellectual Property Litigation & Enforcement
Patents
Trademarks, Copyrights & Trade Secrets
Commercial & Technology Transactions
Cybersecurity & Data Privacy
Advertising & Social Media
Life Sciences & Biotech

Long-Term Actions

Incident response does not end when the impacted system is secured and notification obligations have been met. We also assist clients with respect to longer-term remediation efforts following an incident to improve the security program. Cyberinsurance policies may need to be reviewed. Vendor contracts may need to be evaluated and updated to ensure that appropriate security provisions are in place and that risk is appropriately allocated. Law enforcement and regulators may have questions about the incident and response or may bring enforcement actions. Consumers may file class action litigation, or a customer, business partner or financial institution may file claims in the wake of a data incident. Our highly experienced team is well positioned to provide strategic counsel and representation in those eventualities to help clients achieve the most favorable results.

- Breach coaching/incident response planning
- Breach testing and simulation exercises
- Incident response: investigation, notification, remediation, defense
- Advise on legal obligations arising from incident
- Guidance of forensic investigations
- Draft of notification letters
- Evaluate and advise on proposed insurance policies for privacy and other data incidents