CORPORATE COMPLIANCE INSIGHTS
THE PREMIER GLOBAL NEWS SOURCE FOR COMPLIANCE, ETHICS, RISK & INFORMATION SECURITY

April 2024

Navigating Personal Liability: Post–Data Breach Recommendations for Officers

By Daniel B. Garrie Esq. and Hon. Richard A. Kramer (Ret.)

A data breach doesn't just pose risk to an organization or those whose information was accessed or leaked. Increasingly, regulators and other authorities are signaling their intention to hold company executives liable in many cases. Daniel B. Garrie Esq. and Hon. Richard A. Kramer (Ret.), both mediators with JAMS, offer guidance on navigating the aftermath of a data breach for CSOs and CISOs.

In the interconnected world of digital information, the risk of a data breach has increased exponentially. A data breach can have significant financial, reputational, legal and emotional implications for an organization, its personnel and clients and others. When a data breach occurs, people want to know how it will affect them personally. Not only is their financial well-being at risk, but their privacy has been invaded. Government regulators and politicians often spring into action after a data breach for a wide range of purposes.

For a chief security officer (CSO) and chief information security officer (CISO), a breach presents unique consequences, including potential personal liability. In cases where it can be demonstrated that the CSO or CISO acted negligently or failed in their duties, they could be held personally liable. This could result in financial penalties, disqualification from holding a director or officer position in the future and, in extreme cases, criminal charges.

Upon learning of a data breach, contact your organization's legal counsel; this is the most important action to take in the wake of a breach. A checklist for your initial discussions with the lawyers should include the following:

1. Who in your organization should be advised of the data breach and who, whether or not within your organization, should not.
2. Whether the lawyers can and will be representing you personally as well as your organization and, if not, how you might go about finding counsel.
3. Ask to be educated (or refreshed) on attorney-client privilege. Attorney-client privilege is a critical protection that must be preserved, regardless of whether legal action is taken as a result of the breach.
4. Ask about a litigation hold, which is a directive instructing everyone in your organization to preserve all documents, even those that are normally destroyed in the regular course of business. Counsel will determine the scope of such instruction, but everyone should understand how it applies to their particular role. Nobody wants to be accused of destroying evidence.

5. If you are not the CSO or CISO, ask counsel to contact these people.
6. Ask about documents to be turned over to counsel. This will likely include the materials submitted with the claim by the claimant, documentation regarding the claim that are within your organization, any policy or applicable guidelines regarding data security and any materials already generated or gathered by you.
7. Be prepared to provide counsel with a detailed description of your knowledge of the incident, along with the identification of any other organization-controlled individuals who may be involved and any supporting documentation. Counsel can guide the incident response and provide legal advice to limit both the organization's and your personal liability.
8. Ask counsel about anything else that comes to mind. If it raises your concern, it is worth sharing with counsel.

Counsel will likely ask you to document what you know about the incident and instruct you how to do so. All relevant details are important. These include the date and time the breach was discovered, the nature of the breach, the types of data involved, the number of individuals affected, any immediate steps already taken and anything else that is pertinent.

While the entire scope of relevant information may not yet be apparent, you should err on the side of being more inclusive. Your documentation should be prepared as close in time to the breach as practical to capture your recollections as well as information that may reside in people who could leave the organization. This documentation is critical to help guide internal and external investigations, assist in regulatory compliance and help reduce the impact of potential legal proceedings.

It can be tempting for CSOs and CISOs to take the reins in data breach incidents, given their technical expertise or sense of personal responsibility. However, this can lead to unintended legal complications. In the aftermath of a data breach, it's critical to let your organization's legal counsel guide decision-making processes. They can ensure that the response to the data breach complies with applicable laws and that both communication and remediation efforts are handled appropriately to minimize potential liability.

In addition to protecting the organization, the CSO and CISO may want to seek personal legal advice. Although it's rare to face personal liability or criminal charges, it can happen. Independent legal advice can provide guidance tailored to your specific situation, identify where your interests may be different from those of your organization and allay your concerns — all of which is protected under attorney-client privilege.

After a data breach, effective communication is crucial. Legal counsel should guide the crafting of public statements to ensure they are accurate, timely and compliant with legal obligations. Remember, providing incorrect or misleading information can increase liability risks. Public information can also positively or negatively affect the public's concern over their personal financial and privacy risks. Consult with legal counsel before making any public statements or communicating with affected parties.

Data breaches often involve various regulatory agencies. Cooperate fully with any investigation while also protecting the interests of the organization. This cooperation should be guided by legal counsel to ensure that it does not inadvertently increase liability.

Post-incident, review the causes of the breach and update security measures accordingly. This helps prevent future incidents and demonstrates a commitment to security, which can help limit liability. Legal counsel should be involved in this process to ensure any changes align with regulatory requirements.

Unfortunately, data breaches have become so common that organizations are preparing for when one happens, not if. It is prudent to implement a robust incident response plan (IRP) so it's there when needed. If your organization does not have one, develop one. An IRP can help prevent knee-jerk reactions, demonstrate a good-faith effort to address the situation and provide a solid basis for defense if faced with legal claims.

The key to minimizing personal liability for CSOs and CISOs after a data breach is to act responsibly and reasonably. In order to meet this standard, one should engage with counsel and follow their advice, communicate effectively and demonstrate a commitment to addressing the breach and preventing future incidents. By following these recommendations, CSOs and CISOs can navigate the challenging terrain of a data breach while minimizing their own risk of personal liability.

Anna Diaz Gessner contributed to this report.

Daniel B. Garrie Esq. is a distinguished neutral with JAMS, an arbitrator, mediator and special master with a focus on cybersecurity, data privacy, e-discovery and intellectual property. He is the founder and managing partner of Law & Forensics, where he leads the cybersecurity and forensic practice teams and frequently testifies as an expert witness on e-discovery, cybersecurity and computer forensics. Additionally, he is a fellow of the Academy of Court-Appointed Neutrals. He is also a professor at Harvard in the School of Continuing Education, teaching courses on cybersecurity law, information security and computer forensics.

Hon. Richard A. Kramer (Ret.) serves as an arbitrator, mediator and special master at JAMS in a variety of disputes, including business/commercial, class action/mass tort, construction, employment, environmental, financial markets and insurance. Prior to joining JAMS, Judge Kramer served for nearly 20 years on the San Francisco Superior Court. For 13 years, he presided over cases in the court's complex litigation department.