

Panel Title: Data Breaches: Industry and Law Enforcement Perspectives on Best Practices

Over the course of this one hour presentation, panelists will cover the following subject areas, providing answers and guidance regarding the questions identified in each subject area, as follows:

- Processes/best practices for issuing breach notification. Virtually every state in the United States and several other jurisdictions (e.g. Puerto Rico) require organizations who experience a data breach to notify affected individuals if personal identifying information is compromised. These laws are continually changing, as are the demands and expectations for compliance with these obligations. What are best practices? What are the standards for determining that you have suffered a breach and need to notify individuals? How long can you wait legally to notify, and what are the practical considerations that drive that timeline? Are there instances where you do not have to notify individuals, or can delay notification? What is the role of law enforcement in making that decision, and how can you work with law enforcement regarding breach notification obligations? Can you avoid notification, and what are the legal consequences both in terms of litigation and regulatory enforcement for not notifying individuals? Do any of the laws require organizations to offer services to the victims, and if so what services?
- Consumer victim responses. Breach response is driven in large part by the need to respond to notification requirements, but also to respond to potential litigation and regulatory inquiries. What are the common consumer mistakes that you need to be mindful of in deciding how to respond to a breach and notify customers/individuals? What do the contents of the notice need to say, and should they (or do they have to) make reference to law enforcement efforts or other regulatory agencies? What percentage of customers actually report criminal effects of the breach to law enforcement? Can you change that, or encourage reporting in an effective way? How can law enforcement better facilitate reporting?
- Preparing for and Responding to a Breach. Hackers cannot be stopped, but organizations should prepare themselves by increasing security and formulating a



BREACH INCIDENT RESPON SEqw 0.8385 0j 0.2

Coordinate with Legal Counsel to Bring in Cyber Security Experts and Forensic Examiners

In the rush to mitigate a breach, internal security and IT often are not in a position to verify the depth and extent of a breach, especially when an APT (advanced persistent threat) is involved or the hackers have left "backdoors" to permit subsequent access. Forensic experts, retained and directed by legal counsel, bring independence to investigations, and are free from real or perceived conflicts that might be imputed to internal IT and security personnel who manage the affected systems. Further, by retaining experts via legal counsel, communications prepared for or by the experts can be protected by the attorney-client privilege.

Through counsel, forensic experts can advise your organization how to proceed to stop data loss, secure evidence, and prevent further harm. They are also trained to preserve ephemeral evidence and manage the chain of custody, minimizing the chance that evidence will be altered, destroyed, or rendered inadmissible in court. (S)Tijl-0.004 Tc

Define Legal Obligations

Domestic breach notification laws vary from state to state. In addition, your organization may have notification obligations under the law of other countries if data for non-U.S. individuals was lost. Legal requirements will also vary depending on the types of data, the venues at issue, and the form in which the data is stored. Among other things, these laws affect the timing, content, and form of any required notification. With guidance from counsel, determine whether there are also obligations to notify service providers, payment card networks, or other contractual partners. Additionally, engage counsel to review insurance policies to determine whether insurance carriers should be notified to preserve coverage rights.

Conduct Interviews of
Per



ABO