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 the 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 response plan. How do you begin to prepare an incident response plan? What are the components? How do you formulate your investigative team, and what are the legal and conflict of interest questions to be considered? Are there things that you can do to prevent a breach or make it less likely? How do you decide what vulnerabilities to close, and which ones to leave open? How do you assess legal risk around a technical vulnerability? Can you proactively communication with regulators before there is an incident? Why is that advisable, and how do you do it?

BREACH INCIDENT RESPONSE: AN EMERGENCY PREPAREDNESS GUIDE

A data breach is any unauthorized acquisition or release of, or access to, information, which usually exposes the information to an untrusted environment. Though legal definitions vary, data breaches come in all shapes and sizes, such as files or documents stolen from an office or car; lost laptops, mobile devices, or tablets; compromised servers or e-mail accounts; hacked computers or social media accounts; and APTs (advanced persistent threats).

Data breaches can cost a company millions of dollars in mitigation and remediation costs (an average of $5.4 million per breach in the U.S. in 2011), and cause significant harm to its brand and reputation. The first 24 hours after you discover a breach are critical to restoring security, minimizing harm, obtaining and preserving evidence, and complying with contractual and legal obligations. This checklist provides company executives and in-house counsel with prioritized key steps to take (and not to take) in response to a breach.

Assemble an Incident Response Team (IRT)	The makeup of an IRT will depend upon the kind of breach, what information/data was lost, and what the threat vector was. It may include: An executive with decision making authority; A team leader responsible for response coordination, contacting outside counsel and the forensics team, and addressing press inquiries; "First-responder" security and IT personnel with access to systems and permissions; Representatives from key departments, including IT, Legal, Human Resources, Customer Relations, Risk Management, Communications/Public Relations, Operations (for physical breaches), and/or Finance (for breaches involving loss of company financial information); CIO, CISO, CPO, CITO and/or other C-level stakeholders; and Outside counsel.
Contact Inside and Outside Counsel to Establish a "Privileged" Reporting/ Communication Channel	Establishing a privileged reporting channel (ideally before a breach occurs) maintains the confidentiality of the investigation. Counsel should provide legal advice, retain forensic cyber security experts, and direct response actions every step of the way to protect the confidentiality of the investigation and of applicable internal communications under the attorney-client privilege and work product doctrine. Consider emphasis on use of telephone for critical and sensitive communications in the event that e-mail and electronic communications channels may be compromised. Counsel should also be involved in the establishment of the investigative team and receive all incident reports (initial, draft, and final), including IT-related communications, for the purposes of providing legal advice. Outside counsel can also work (and have established relationships) with law enforcement and forensic experts who can assess risk and provide guidance on remediation, disclosure, and notification efforts.

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.
Stop Additional Data Loss	If the breach is ongoing, consult with forensic experts, trained IT staff, and security personnel about taking affected systems offline by disconnecting them from the network and/or using tools to dynamically image affected systems to preserve evidence. If paper records or other physical assets were compromised obtain tracking information, logs, and surveillance evidence, if available.
Secure Evidence	Secure and prevent physical access to affected systems, such as servers and workstations, to maintain the integrity of the evidence and ensure that only selected forensic experts and law enforcement (if applicable) have access. Preserve all security access device (token, key card, building credentials, etc.) logs and surveillance tapes. Work with counsel to send preservation letters to service and cloud providers. Track the chain of custody (i.e., who had contact with the affected system, what did they do, and who was the next to touch the affected system) for all physical or digital evidence. Inventory any missing hardware. If the compromise occurred on vendor's computer systems, or was the result of a vendor's loss of paper, media, or data in other traditional physical forms, request retention and copies of relevant evidence, such as forensic server images, logs, tracking information, video surveillance, and e-mail.
Preserve Computer Logs	Preserve all affected system log files, including firewall, VPN, mail, network, client, web, server, and intrusion detection system logs. These logs are critical to assessing the origins of the attack, its duration, and volume of data exfiltrated during the breach.
Document the Breach	Record the date and time of the breach, the personnel who discovered the breach, the nature of the breach, the kinds of data stolen/lost, when the response efforts began, and all of the employees who had access to the affected systems. Document all data and/or devices and hardware lost in the breach. Because a high percentage of data breaches can be traced to former employees, obtain names and contact information for all employees terminated within the last 90-120 days, and confirm that their security access has been terminated.
Contact Law Enforcement (Possibly)	After consultation with legal counsel and upper management, determine whether contacting law enforcement is necessary (especially where E.U. "data subjects" are involved), prudent, and/or valuable. In some cases, but not all, you may be able to delay notification requirements if it would impede or interfere with a law enforcement investigation. Law enforcement's expertise in evidence gathering and forensics can be leveraged to ensure that the evidence can be used in future court proceedings.

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 Personnel Involved	Identify all of the individuals who were involved in the discovery and initial investigation of the breach. Conduct interviews to create a complete record of all efforts taken to stop data loss, secure systems, mitigate damage and harm, etc. Determine whether counsel (inside or outside) should participate in the interviews and be present if law enforcement also requests interviews with relevant personnel.
Reissue or Force Security Access Changes	Increasingly, cyber criminals are after log-in credential and password combinations. After a breach, personnel should be required to change passwords and be issued new physical authentication/access devices (tokens, badges, key cards, etc.). Because intruders are often after the personally identifying information of employees, as well as customers, these same personnel should also be strongly encouraged to change passwords for their personal banking, healthcare, web mail, and social media account passwords.
Do Not Probe Computers and Affected Systems	Evidence could be accidentally altered or lost, or intruders could be alerted to your activities, causing them to take measures to hide their trail, damaging your systems in the process.
Do Not Turn Off Computers and Affected Systems	Valuable information can be stored in temporary memory storage spaces that could be lost if you unnecessarily turn off a running system. If an affected system is on and/or connected, leave it on and connected. Work with forensic experts to determine whether the system should be dynamically imaged before disconnecting it to avoid tipping cyber criminals to the fact that you are aware of the breach and to preserve evidence that they might otherwise destroy to conceal their tracks. If the system is off, unplug it.
Do Not Image or Copy Data, or Connect Storage Devices/Media, to Affected Systems	Imaging and copying of affected systems should be left to forensic experts and law enforcement agents who are equipped with state-of-the-art forensic toolkits and imaging utilities. Copying data without the right protocols and tools (even for the purpose of providing to law enforcement) can alter or destroy important evidence, and render evidence inadmissible in court.
Do Not Run Antivirus Programs or Utilities	Running programs or utilities on the affected systems could result in the accidental loss or destruction of evidence.
Do Not Reconnect Affected Systems	Affected systems should be preserved until forensic or law enforcement examination and remediation efforts have been completed. A "cleaned" system is not always clean. Backdoors and persistent threats are designed to lull personnel into a false sense of security. All affected systems should go through rigorous testing and verification before being reconnected to the network.

ABOUT US

DLA Piper is a global law firm with lawyers across the Americas, Asia Pacific, Europe and the Middle East.

From the quality of our legal advice and business insight to the efficiency of our legal teams, we believe that when it comes to the way we serve and interact with our clients, everything matters.

FOR MORE INFORMATION

A data breach places you and your organization in crisis management mode. While the crisis cannot be averted, your organization can plan for it. Organizations who work with counsel to create a pre-breach incident response plan can save millions of dollars and significant reputational harm. DLA Piper LLP (US) can help. For more information on data breach incident response planning, please contact:

Aravind Swaminathan
Partner
T +1 206 839 4835
C +1 206 639 9157
aravind.swaminathan@dlapiper.com

Jim Halpert
Partner
T +1 202 799 4441
C +1 202 276 5476
jim.halpert@dlapiper.com

Stef Fogel
Partner
T +1 617 406 6053
C +1 215 356 7589
stefanie.fogel@dlapiper.com

Jennifer Kashatus
Of Counsel
T +1 202 799 4448
C +1 202 421 4321
jennifer.kashatus@dlapiper.com

www.dlapiper.com