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: paper files or documents stolen from an office or car; lost laptops, mobile devices or tablets; compromised servers or email accounts; hacked computers or social media accounts; or APTs (advanced persistent threats).

Data breaches can cost a company millions of dollars in mitigation and remediation (in 2011 in the US alone, an average of $5.4 million per breach), while causing significant harm to 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 • Outside counsel.
Contact inside and outside counsel to establish a "privileged" reporting and 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 cybersecurity experts and direct responses 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. Counsel should also be involved in establishing 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 cybersecurity 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 themselves back doors to give themselves future 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.
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 (tokens, key cards, building credentials) 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? Who was the next to touch the affected system?) for all physical or digital evidence. Inventory any missing hardware.
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 EU "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 other the law of other countries if data for non-US 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 and mitigate damage and harm. 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, cybercriminals 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). 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, health care, web mail and social media accounts.

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.

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 can help. For more information on data breach incident response planning, please contact:

Stefanie Fogel
Partner
C +1 215 356 7589
stefanie.fogel@dlapiper.com

Tara Swaminatha
Of Counsel
T +1 202 799 4323
tara.swaminatha@dlapiper.com

Jim Halpert
Partner
T +1 202 79 4441
C +1 202 276 5476
jim.halpert@dlapiper.com

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

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.

www.dlapiper.com