

Top 10 Data Breach Questions for Your Organization

Shed some light on undiscovered risk.

1. Was any data compromised?

When it comes to a data breach, initial assumptions can be misleading. Kroll can assist you in determining whether data was actually lost or subjected to unauthorized access.

2. What data was really compromised?

Through forensic analysis, data review services, and more traditional investigative techniques like interviews, Kroll will help you establish the universe of data that was compromised. Sometimes, that universe is significantly smaller than initially thought, substantially reducing your legal, regulatory, and reputational exposure.

3. Is the data breach still occurring?

Organizations that have experienced a data breach sometimes assume that intrusion events are discrete, one-time incidents, as opposed to active and ongoing policy violations, employee error, or criminal conduct. The consequences of mistaken assumptions can be devastating. Kroll's forensic and technical investigation experts can help you eliminate the uncertainty by determining whether a data breach may be ongoing and then identifying the appropriate steps you should take to "stop the bleeding."

4. Have you set a defensible path?

When a data breach is suspected, first responders may unknowingly damage or destroy information that is critical to investigation or litigation, should that later be indicated. Early involvement of a third-party forensics team like Kroll's, which understands both security and discovery protocols, can help determine how to collect and preserve evidence and information in the process of containing the event.

5. Was the data breach accidental or malicious? Who is responsible?

Kroll's powerful fact-finding capabilities can assist you in investigating who may have been responsible for the theft of a laptop, a break-in, a hacking event, or virtually any form of data breach. In some cases, through investigative techniques and resources, Kroll can even secure the return of a device containing sensitive data and establish the extent to which the data may have been disseminated.

6. What about encryption?

The need for encryption should be assessed both for sensitive data at rest and sensitive data in transit. The need is particularly acute for users of laptop computers and other portable devices and storage mechanisms. Take note that many laptop systems won't encrypt the data until the machine is shut off—closing the cover with the computer still running won't do the trick! What about external storage devices like USB hard drives, flash memory sticks, and backup tapes? Are they encrypted? Aim for 100% encryption of sensitive data on all portable media.

7. Have you implemented a crisis communications plan?

Even before the scope of an event can be determined, questions will inevitably emerge, from both internal and external sources. Rumors, confusion, and inaccurate information can damage reputation and brand. Once the incident is known, a communications team should be designated to establish procedures for delivering accurate and timely information in a clear, concise, and consistent manner.



Top 10 Data Breach Questions

8. Have you alerted your outside counsel?

Outside counsel with privacy law expertise affords the latest guidance in this ever-changing and relatively young discipline of law. You and your outside counsel may determine that your outside counsel will retain any investigation or forensics work so that the work may be subject to attorney work product protection and the attorney-client privilege, to the extent applicable. Kroll is a leading provider of technical investigation and electronic discovery services and consulting and has unparalleled experience working with corporations and their outside counsel to meet the needs of an investigation or litigation matter.

9. Have you researched your legal obligation for breach notification?

Currently, the process for breach notification is governed by a patchwork of state laws and one overarching federal requirement for HIPAA-covered entities. In some cases, these laws have conflicting requirements. Outside counsel can be quite helpful in assisting with drafting notifications for affected individuals, as well as agency notifications to attorneys general, regulators, media, and stakeholders.

10. Have you tested your data breach response plan?

Mandates like the Red Flags Rule require certain organizations to have a formalized, written plan in place to “detect, prevent, and mitigate” identity theft. A data breach response plan helps answer the mitigation element—provided it is tested regularly and proven to perform as effectively in action as it does in concept. Kroll’s global experience in data breach response on a vast variety of incidents can be leveraged to support you in the development of or improvements to your data breach response policies and plans.

Bonus Question: Can future data breaches be prevented?

Assessing the effectiveness of your security technology and policy adherence is critical. Kroll can conduct a comprehensive risk assessment to ensure that security programs are up-to-date and working properly.

Central to this assessment is helping you identify where your organization’s sensitive data resides and how it is stored and accessed, a process known as data mapping. Kroll can help identify gaps and potential risks in your data security and privacy practices and provide recommendations to prioritize and resolve data security risks based on your organization’s unique data security and privacy needs.



For more information, call or visit us online.

866.419.2052

www.krollfraudsolutions.com

Certain Altegrity companies provide investigative services. State licensing information can be found at www.altegrity.com/compliance. These materials have been prepared for general information purposes only and do not constitute legal or other professional advice. Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have. © 2011 Kroll, Inc. All rights reserved. Item #THT-007-2011-0509