Data Incident Investigation and Breach Response

A proven solution.

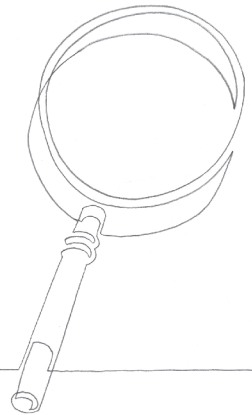
Data breaches take many forms. External hackers and malicious insiders cause many breaches, but did you know that simple carelessness is responsible for a surprisingly large number of breaches?

Breaches can pose a real threat to the individuals whose personally identifiable information has been lost or stolen. Some suspected breaches prove on investigation to be false alarms, but the forensic costs of establishing this can be high. Industry characteristics are critical too – a loss of medical records from a hospital poses different risks from a loss of credit card information from a retailer.

In each case BBR Services collaborates with you to establish the best response that is tailored to your individual needs.

Case studies

- When the HR director of a financial institution noticed fictitious users in their payroll system and it looked like hackers also gained access to their customer database, BBR Services jumped in and guided the bank through the entire breach response process, from lining up experienced privacy counsel, through the complex and detailed forensic investigation, as well as the coordination of the notification process to the thousands of individuals within the bank's customer database.
- An online electronics retailer had no idea what to do when it received a letter from its bank advising of $500,000 in fraudulent charges from 455 cards made on the retailer's website, and instructing the retailer to immediately commence an investigation and hire a Payment Council Industry (PCI) approved forensic investigator within 48 hours. They called BBR Services and that same day BBR Services formulated an investigation and response plan, lined up a leading PCI-approved forensic investigator within 24 hours, and connected the retailer with breach response counsel specialising in PCI compliance. The forensic investigator determined that no breach had occurred on the retailer's end and, based on this, the bank and credit card company both closed their investigations.



Case studies

- A physician practice discovered that its entire computer system, including its electronic medical record platform, had suddenly become unresponsive. Multiple attempts to log on to the system failed. The practice then received an email from an unidentified individual, explaining that the sender had hacked their network, encrypted all information on the system, and would only decrypt the information for ransom payment. The doctors were ready to make the payment, but contacted BBR Services first. BBR Services immediately formulated a response strategy: engaging expert breach response counsel and coordinating with the FBI. The FBI and counsel explained that the attacker had a pattern of simply taking the ransom money, reneging on the agreement, and delivering additional malware onto the system. BBR Services helped coordinate the services the doctors needed in order to move forward and notify thousands of patients, federal regulators and the media about the incident.
- When a student mailing sent by a major university inadvertently included 22,000 students' Social Security numbers on the address labels, the university turned to Beazley for assistance. In addition to coordinating the full breach response, including legal, notification and call centre vendors, BBR Services also arranged, through our preferred relationship with Experian, for students without credit files to receive special monitoring by Experian. The result was that students who were not otherwise eligible for credit monitoring were given a tailored solution meeting their needs.
- An identity theft ring operating from Malaysia and Russia assembled profiles on senior physicians at large hospitals. The ring used publicly available information on LinkedIn, as well as Google references to the physicians' attendance at conferences, to construct these profiles. The ring then deployed a spear-phishing campaign with artfully crafted emails targeting the physicians and asking them to reset certain HR information. A number of the physicians clicked an embedded hyperlink in the email. The link captured HR portal log-in information, which the attackers used to divert pay cheques to an offshore account, and allowed the attackers to deploy sophisticated malware on the respective hospitals' systems. Multiple hospitals reported the event to Beazley. BBR Services was able to coordinate and leverage resources for these hospital clients in a manner that significantly drove down response costs for the ensuing forensic and legal investigations.
- A hotel management company had servers located in multiple locations. One of these servers was infected. They called Beazley on a Friday night and forensics had a plan in place by Saturday. They acted quickly and controlled the situation and it was determined no data was breached.

Responding to a breach can be complicated and costly. Working with our experienced BBR Services team, your organisation is guided through and empowered with the resources you need to implement a sound and strategic breach response plan.

beazley