Financial Institutions

Effective data breach protection for financial institutions.

Essentially, a data privacy breach is not a question of "if". The only question is "when?"

Financial institutions' information exposures have many causes and are difficult to control. And even with the best systems, controls, personnel and procedures, no bank or credit union is immune to the risk. It only takes one small human error, or an office break-in, or a clever hacker to compromise millions of records and create havoc within your organisation.

Significant exposure

Regulatory requirements in the event of a data breach vary greatly from one country to another. However, regardless of the differences in legal requirements the ethical issues surrounding financial institutions' data policies are increasingly the subject of close scrutiny. High ethical standards are important to customers and negative publicity around a poorly handled data breach can ruin a bank or other financial institution's reputation in an instant. This requires a holistic approach to risk mitigation that is more than just financial.

The publicity fallout from a data privacy breach entails the risk of massive reputational and brand damage. It is safe to assume that poorly handled breaches result in far higher customer defection rates; in fact, brand value and reputation have been shown to decline by between 17% and 31%* after a mismanaged breach, and it can take upwards of a year to restore an organisation's reputation.

*Source: EIU Global Study, March 2013

378.8m

personal records compromised between 2005 and 2015 were entrusted to financial institutions.
Source: www.privacyrights.org

Financial Institutions

Regulatory investigations and penalties

Compliance with the UK's Data Protection Act (DPA) is not just about the confidentiality of personal data, it is also about information security and ensuring that data is securely stored and managed.

The Information Commissioner's Office (ICO) has several options when it finds that an organisation has breached the UK Data Protection Act. A significant breach of personal data could result in actions including issuing monetary penalties, enforcement notices, auditing and prosecutions.

If an organisation fails to comply with data protection regulation the consequences can be severe, from reputational and share price damage, to hefty fines up to £500,000 and even criminal charges.

Why Beazley

Beazley, a leading insurer of technology and information security risks, has developed Beazley Breach Response (BBR), a solution to privacy breaches and information security exposures tailored to the needs of financial institutions.

BBR is a complete privacy breach response management and information security insurance solution which includes a range of services designed to help you respond to an actual or suspected data breach incident effectively, efficiently, and in compliance with the law.

Beazley understands the maze of data protection regulations faced by financial institutions; we have helped many financial institutions with data breaches related to network intrusions, lost and stolen laptops, inadvertent postings of customer's personal data on web pages and rogue employees stealing customer information.

44%

of customer accounts have been compromised

Source: March 2014 ACI Worldwide survey from BAI Payments

Third party coverage

- Third party information security and privacy coverage with up to €25m/£15m in limits in addition to the breach response coverage
- Regulatory defense and penalties
- Website and offline media liability
- PCI fines, penalties and assessments*
- Cyber extortion
- First party business interruption and data protection with limits up to €25m/£15m.

* Where insurable by law

beazley

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?

Every breach is different. It is important to work with a partner who has been there before.

BBR Services

Beazley is unique among insurers in having a dedicated business unit, BBR Services, that focuses exclusively on helping clients manage data breaches successfully. In each case BBR Services collaborates with you to establish the best response that is tailored to your individual needs.

BBR Services is a dedicated team of data breach professionals who assist BBR policyholders at every stage of incident investigation and breach response.

They coordinate the carefully vetted forensics experts and specialized lawyers to help you establish what's been compromised; assess your responsibility; and notify those you have to. In addition, BBR Services coordinates credit or identity monitoring for your customers and PR advice to help you safeguard your reputation.

Hacking and malware

- A financial services firm reported that the passwords for a web based dealer portal, which was licensed from a 3rd party vendor, were compromised. Four dealer accounts were hacked and the routing and account numbers were transposed. This caused the firm to issue unauthorized deposits to dealers who did not actually request them. BBR Services connected the firm with panel privacy counsel and a forensic firm. After an investigation, counsel determined that the firm was required to notify approximately 600 individuals. BBR services connected the firm with a notification and call centre vendor and helped the firm order credit monitoring codes for affected individuals.

- A bank experienced a sophisticated malware attack, where hackers were in their system for at least six months. The hackers set up fake accounts and money was withdrawn from the bank from those fake accounts. The forensic investigation was extremely expensive due to type of malware. Together with BBR Services, the bank notified and provided credit monitoring to nearly 30,000 individuals whose credit card numbers, social security numbers and driver's license numbers may have been exposed.

- An insurance company's claims management software developer's subcontractor stored data insecurely and a white-hat hacker was able to access the information. The hacker reported the incident to authorities. The vendor investigated and determined that based on the log data, it did not appear that the data was otherwise accessed. BBR Services connected the company with privacy counsel, who advised that notification was required to 20 individuals and one state attorney general.

Financial Institutions

Learn more:
www.beazley.com/bbr

- A financial firm's systems were potentially compromised due to a spear-phishing scheme that resulted in a fraudulent wire transfer and potential exfiltration of emails with customer personally identifiable information (PII). BBR Services recommended forensics and privacy counsel, and they concluded (after an extensive manual review of data) that the insured was legally obligated to notify approximately 3,000 individuals.

Portable device

- An employee had an unencrypted laptop stolen from her automobile. BBR Services quickly connected the company with forensics to assist with assessing the information on the laptop. Once that analysis was complete, the organisation learned that the laptop had contained protected information on approximately 6,000 individuals. BBR Services continued to assist by coordinating notification and call centre services, as well as credit monitoring, for the affected individuals since the laptop contained their social security numbers.

- A financial institution discovered two backup tapes were missing. Forensics evaluation uncovered the tapes contained PII for 84,000 individuals. BBR Services coordinated a response, including notification and call centre services for all affected individual

Payment card fraud

- Credit cards issued by a bank were used to make fraudulent cash withdrawals at various ATMs as the bank's vendor reset the personal identification numbers for the fraudsters without proper credentials. BBR Services connected the bank with privacy counsel to analyze the incident. The bank was pleased with privacy counsel and engaged them separately to go after the vendor for losses.

"During Quincy Credit Union's recent ATM skimmer incident, Beazley Group provided significant assistance in dealing with the many issues involved. When notified, Beazley promptly responded with recommendations for legal assistance and investigative services. This unfortunate occurrence caused great stress and concern on the part of QCU's management team and Directors. Beazley's representatives provided significant support to assist us. I sincerely thank them for their help and highly recommend Beazley's Breach Response Insurance coverage for all credit unions."

Stewart A. Steele, Chief Executive Officer
Quincy Credit Union

beazley