Financial Institutions

Effective cyber breach protection for financial institutions.

Essentially, a cyber 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 potential havoc within your organisation.

Significant exposure

Regulatory requirements in the event of a cyber 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 cyber 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 cyber 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, 22% of breached organisations lost customers and 40% of those organisations lost more than a fifth of their customer base.

Source: Cisco 2017 Annual Cybersecurity Report

643.8m

personal records compromised between 2005 and 2018 were entrusted to financial institutions

Source: www.privacyrights.org

Regulatory landscape

The European General Data Protection Regulation (GDPR) is one of several recent global, legal and regulatory developments that impose significant new data privacy compliance and reporting obligations on organisations that manage personal data.

The GDPR introduced mandatory data breach notification obligations and expanded the regulators' authority and control, including the ability to levy significant fines. The GDPR also opens up the potential for class action style privacy claims throughout Europe, not just for financial losses but also for mental distress. Countries such as Australia, Brazil, Israel, Mexico, the Philippines, South Africa and South Korea are following Europe's lead and are implementing data privacy laws that are more robust.

These new laws and regulations present complex challenges to organisations in terms of what measures they need to implement in order to protect information over which they have custody. Responding effectively to incidents that affect this data and mitigating the potential costs and impacts of the incident is now a critical concern.
.

60%

of financial institution breaches in 2018 were attributed to hack or malware

Source: Breaches reported to BBR Services

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 cyber 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 cyber breaches related to network intrusions, lost and stolen laptops, inadvertent postings of customers' personal information on web pages, and rogue employees stealing customer information.

Coverage

Breach response
- Legal services
- Computer forensic services
- Notification services for up to five million affected individuals
- Call centre services
- Credit monitoring, identity monitoring or other personal fraud or loss prevention solutions
- Public relations and crisis management expenses
- All of the policy's multiple limits will be available for breach response.

First-party
- Business interruption loss from security breach or system failure
- Dependent business interruption loss from security breach or system failure
- Cyber extortion loss
- Data recovery loss
- Data and network liability.

Third-party
- Third-party information security and privacy coverage up to £15 million
- Full media liability
- Regulatory defence and penalties
- Payment card liability and costs.

Criminal reward

Cyber 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 cyber 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 specialised 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 offers PR advice to help you safeguard your reputation.

BBR Services also provides a full range of resources to help mitigate risks before an incident occurs. On our Beazley owned and managed risk management portal, global.beazleybreachsolutions.com, you will find resources for incident response planning, employee training, compliance, and security best practices. Newsletters and expert webinars educate you about the latest threats, preventive steps, and regulatory developments. BBR Services also coordinates a variety of pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops, so you can improve the robustness of your cybersecurity.

Case studies

Hacking and malware

- A financial services firm reported that the passwords for a web-based dealer portal, which was licensed from a third-party vendor, were compromised. Four dealer accounts were hacked and the routing and account numbers were transposed. This caused the firm to issue unauthorised 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 the 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 licence numbers may have been exposed.

Case studies

- 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.
- 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 back-up tapes were missing. Forensics evaluation uncovered the tapes contained personally identifiable information (PII) for 84,000 individuals. BBR Services coordinated a response, including notification and call centre services for all affected individuals.

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 analyse 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