Retail

Effective cyber breach protection for retailers.

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

Information exposures are difficult to control and are subject to many different types of loss event. And even with the best systems, controls and personnel, no retailer is immune to the risk. It only takes one small human error, a simple property crime, or one clever hacker, to compromise millions of customer records.

Significant exposure

Retailers are prime targets for cyber criminals, as retailers transmit and store large amounts of consumer and employee information, including credit card data. Point-of-sale systems are an easy entry point, especially if point-to-point end encryption is not implemented properly. Once such a breach occurs, compulsory data breach notification laws will ensure that the public knows about the event, posing a significant risk to the retailer's reputation and brand.

Payment Card Industry (PCI)

Commerce without credit and debit card payments is unimaginable. Whether at the point of sale, online or through a call centre, the retail industry processes a staggering volume of credit card transactions. A breach of credit card information, which the card brands frequently detect before the organisation even suspects any foul play, can result in fines, penalties, mandated computer forensic costs, legal fees, and worst of all, the inability to process payments.

1.4bn

personal records compromised in retail between 2005 and 2018

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.

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 retailers.

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.

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.

eCrime
- Fraudulent instruction
- Funds transfer
- Telephone fraud.

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, 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 retail chain received common point-of-purchase notices from card brands indicating suspected fraud stemming from their organisation. Because a PCI forensic investigator (PFI) was mandated, BBR Services connected the organisation with a PFI that undertook an investigation of their network, as well as with legal experts to provide counsel at every step of the way. The forensic investigation discovered malware, and a second forensic investigator was retained to perform a separate portion of the investigation. BBR Services also assisted with a call centre as well as crisis management services.
- A fashion retailer received a common point-of-purchase notice for one of its chain store locations. BBR Services quickly connected the organisation to a forensics firm and privacy counsel. After further investigation, the retailer discovered a skimmer on one of its registers. Forensic analysis revealed that some card information had been accessed during a short window of time. The retailer provided substitute notice through its website.

Case studies

- Malware on a retailer's point-of-sale system was believed to have compromised 150,000 to 200,000 payment cards. BBR Services arranged panel counsel and a forensic firm for the retailer. After the forensic investigation, the retailer notified and provided credit monitoring to 100,000 affected individuals. The notification vendor was able to operationalise a call centre and a credit monitoring offer for over 100,000 people within 48 hours from the notification. The retailer also used crisis management services to assist with the breach.

Portable device

- An incident arose when a laptop was stolen from a vehicle being used by a retailer's human resources manager. The laptop was unencrypted and held files containing employee information, such as name, address, Social Security number and salary information, for all the company's employees from 2004 to 2008. Forensics and privacy counsel were engaged and determined the retailer was obligated to notify and provide credit monitoring to 36,000 individuals.

Distributed denial of service (DDoS)

- An online retailer who generates a large amount of revenue per week on their website had a major outage, causing the website to be down for one hour. The retailer received subsequent emails from a well-known DDoS gang threatening to return Monday morning with a larger attack, which would bring them down for six hours unless they received 30 Bitcoins. The retailer called BBR Services late at night on a weekend. BBR provided guidance and arranged services for the retailer to help them in the event of a larger attack. The retailer quickly retained a mitigation service and was not impacted by the larger incident.

"The response from the Beazley Group after discovering a potential data breach was an amazing demonstration of customer service and professional guidance. The response time was fast, less than an hour before the team was pulled together for a teleconference with our representative and we were issued next steps within an hour after that. Having Beazley in our back pockets has already paid for itself three-fold and in my opinion is essential for any business continuity and disaster recovery plan."

Sonya Lynn, EVP, Chief Operating Officer
Craft3

beazley