Retail

Effective data breach protection for retailers.

As thousands of retailers, large and small, have learned to their cost, a data 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 events. 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.

257.5m

personal records compromised in retail between 2005 and 2015

Source: www.privacyrights.org

Significant exposure

Retailers are prime targets for cyber criminals looking to exploit vulnerabilities through point of sale systems. 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. A study conducted by the Economist Intelligence Unit in April 2013 found that 38% of respondents affected by a data breach no longer did business with the organisation concerned "because of the data breach," and 46% said they had advised friends and family to be careful of sharing data with the organisation.

Payment Card Industry (PCI)

Commerce without credit and debit card payments is unimaginable. Whether at the point-of-sale, online, or through a call center, 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.

Retail

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 and even criminal charges.

In 2015 fines imposed by the ICO totalled over £1.1 million.*

*Source: www.ico.org.uk

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 data breach incident effectively, efficiently, and in compliance with the law.

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

88%

of records breached in 2014 were attributed to retail data breaches

Source: www.privacyrights.org

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 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.

- Malware on retailer's point of sale system was believed to have compromised 150,000 - 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.

Retail

Learn more:
www.beazley.com/bbr

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 of the company's employees from 2004 - 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 1 hour. The retailer received subsequent emails from a well-known DDoS gang threating to return Monday morning with a larger attack which would bring them down for 6 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