First-Party Computer Claims

Beazley provides valuable first-party computer coverage for business interruption, cyber extortion and data protection losses.

The Beazley difference

Collaborative
We work with you as a team through each step of the claim to find the best possible outcome.

Experienced
The professionals on our claims team, most of whom are former senior litigators, understand the emerging liabilities and complexities of the cyber world.

Accessible
You work directly with a claims manager who is empowered to make decisions and resolve complex claims.

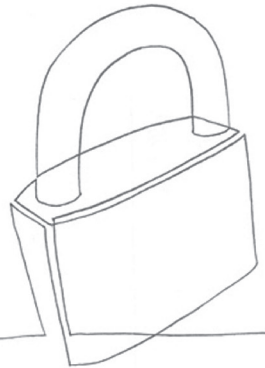
Pragmatic
We take a practical, real-world approach to managing claims rather than "ticking boxes." We understand that no two claims are alike and each claim presents unique challenges requiring individualized case strategies.

Flexible
We can support you in handling incidents in-house, or can work cooperatively with any third-party privacy counsel, forensic experts and consultants you retain.

Consistent
You will work with the same Beazley claims manager throughout the entire life of the claim: validating coverage, analyzing the claim, assessing liability and developing a strategy to obtain the best possible result for your business. Your claims manager will work side by side with you until the claim is resolved.

Hacking and malware attacks are on the rise. In 2018 47% of breaches were attributed to hacking and malware, compared to 32% in 2016.

Breaches managed by Beazley Breach Response Services



Beazley has paid out several million dollars in first-party cyber coverage claims, including the following examples.

Case studies

Business interruption

- A global marketing firm that operates promotional websites for its clients, and collects personal and financial information from clients' customers through these websites, discovered that it had been breached. A forensic investigation revealed that foreign code embedded on the website was sending customers' credit card and identifying information to unidentified unauthorized recipients, compromising more than one million records. Beazley worked with the firm and privacy counsel to mobilize resources to respond to clients, customers and relevant data protection authorities. Beazley quickly approved the engagement of privacy counsel in multiple jurisdictions, forensic experts and PR consultants. Beazley worked with the firm to agree to a commercially reasonable format for submission of proof of loss and paid more than $1 million in business interruption (BI) loss.
- An online retailer experienced a distributed denial of service attack (DDoS) on its website and backend computer systems. The sophisticated attack lasted over a number of days during an important holiday shopping season. The DDoS was made with the intention to extort the retailer, but the insured decided not to pay the ransom. Beazley worked closely with the retailer, an outside forensic accounting firm and the broker's forensic accounting department. Beazley paid the retailer over $1 million in BI loss.
- A retailer experienced a DDoS attack on its website. During the attack, which lasted several days, the retailer experienced a significant decrease in online sales, though it received no extortion demand. No personally identifiable information (PII) was involved. The retailer engaged a DDoS mitigation expert when it could not resolve the issue internally. Beazley worked closely with the retailer (including several in-person meetings) after the matter was reported to evaluate the claim, and paid the retailer over $300,000 in BI loss.
- An accounting firm suffered a crypto-malware attack during its busy season. The malware spread from one of the firm's local computers to its network, encrypting data in the process and making it inaccessible to the firm's employees. The firm disconnected all machines from the network to halt the spread of the virus, while the firm investigated the cause and extent of the intrusion and then restored compromised data. Employees of the accounting firm were not able to perform client work until the data was recovered and the network restored. After the firm submitted a proof of loss quantifying the BI loss, Beazley paid over $40,000.
- A crypto-malware attack infected the computer network of a law firm, encrypting the firm's data and files. All machines, including the server, were disconnected from the network to block the malware from spreading. This small family-owned law firm was unable to perform client work for days while the network was down. Beazley paid over $5,000 in BI and data protection losses.

Cyber extortion

- After a DDoS attack that forced an online retailer to take down its website, the retailer received a demand from the hacker for several thousand dollars in Bitcoin, threatening a larger DDoS attack if the retailer did not pay. Rather than pay the monetary demand, the retailer purchased upgraded DDoS protection services in response to the threat. Beazley paid over $60,000 in cyber extortion loss.
- An online jewelry retailer was threatened with a DDoS attack if it did not pay a Bitcoin ransom. The retailer refused to pay the ransom and instead retained a security consultant with Beazley's consent to provide enhanced DDoS mitigation in connection with the threatened attack. Beazley paid over $40,000 in cyber extortion loss.
- An online apparel retailer was threatened with a DDoS attack if it did not pay a Bitcoin ransom of several thousand dollars. The retailer paid the ransom with Beazley's consent and retained a security consultant to provide DDoS mitigation. The retailer incurred tens of thousands of dollars in addition to the ransom amount. Beazley paid over $10,000 in cyber extortion loss.

Data protection loss

- An international software company suffered a malware attack affecting dozens of servers, desktops and laptops. The company incurred significant amounts in external forensic costs investigating the scope and impact of the attack, recovering data and restoring impacted systems. Beazley reimbursed the company over $800,000 in data protection loss and privacy breach costs.
- A public entity suffered a security breach that took down all systems. The organization incurred substantial costs in response to the downtime and suffered significant data loss. Beazley reviewed and adjusted the organization's proof of loss, paying over $190,000 in BI and data protection losses.
- A healthcare organization's offices in Phoenix, Chicago and Nashville were affected by the Pink Slip virus. Forensic investigators determined that protected health information and personally identifiable information were not compromised by the incident. Unfortunately, the healthcare organization incurred data losses and expenses in responding to the virus, and Beazley paid over $120,000 in data protection loss.

BZCER001_US_01/19