Professional Services

Effective cyber breach protection for professional services firms.

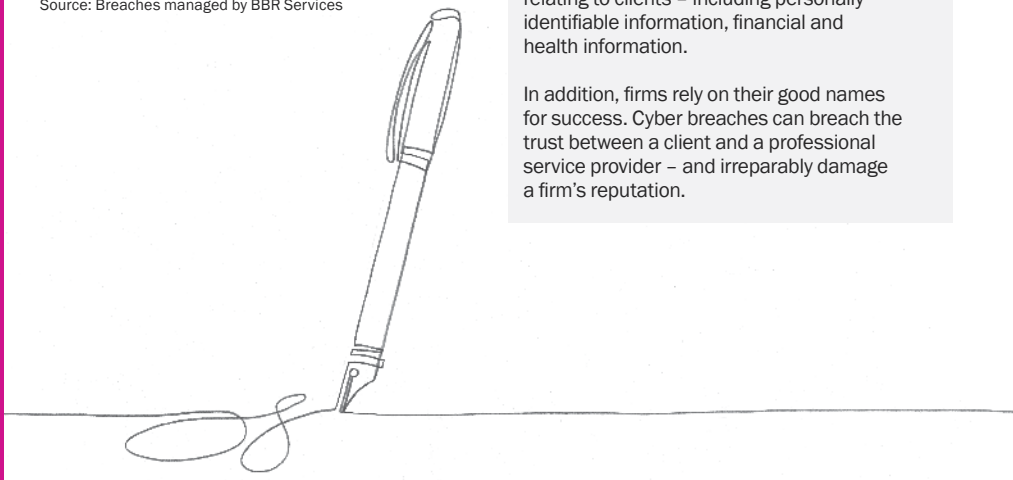
Essentially, a cyber breach is not a question of "if." The only question is "when?"

Information exposures are difficult to control and subject to many different types of loss events. Even with the best systems, controls, personnel and procedures in place, no professional services firm is immune: It only takes a small human error, one lost laptop, or a clever hacker to compromise client records and wreak havoc on your organization.

60%

of breaches Beazley managed for professional services firms in 2016 arose from hacking or malware.

Source: Breaches managed by BBR Services



Significant exposure

Clients entrust professional services firms with the most sensitive information about themselves and their family members, including financial and investment data, tax returns, personal and business income figures, privileged legal information, estate planning materials, Social Security numbers, and driver's license numbers and other governmental identification numbers. This information is highly attractive to hackers and vulnerable to breaches both accidental and malicious.

Professional services firms – which include accountants, tax preparers, lawyers, financial advisors, insurance agents and real estate brokers – commonly have fewer resources than larger companies to devote to managing and mitigating cyber vulnerabilities. When a breach occurs, firms can be obligated to comply with complex state privacy notification laws, undertake time-consuming internal forensics, and face outside regulatory investigations and liability claims. For some professional services providers, attorneys for example, the bar is even higher. They have contractual and regulatory obligations to protect information relating to clients – including personally identifiable information, financial and health information.

In addition, firms rely on their good names for success. Cyber breaches can breach the trust between a client and a professional service provider – and irreparably damage a firm's reputation.

Professional Services

Class action lawsuits

The publicity and customer dissatisfaction that surround a cyber breach have spurred a wave of class action complaints against professional services providers big and small. Enterprising plaintiffs' lawyers relying on a variety of privacy laws have filed complaints seeking billions in damages. The risk of crippling damages, and the sizeable costs of litigation, often push organizations to settle even in the absence of any clear harm to the plaintiffs.

Regulatory investigations and penalties

State and federal regulators have made one point clear: A significant breach of customer information will result in monetary penalties, onerous corrective action plans, and on-going audits. Whether from the Federal Trade Commission or state attorneys general, the regulatory landscape surrounding data breaches carries an immense amount of risk.

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 professional services firms.

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 professional services providers. We have helped many firms with data breaches ranging from network intrusions and lost laptops, to inadvertent postings of customer Social Security numbers on web pages and rogue employees stealing client information.

Coverage

Breach response

- Legal services
- Computer forensic services
- Notification services for up to 5 million affected individuals
- Call center 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 coverage

- Third party information security and privacy coverage with up to $15M
- Full media liability
- Regulatory defense and penalties
- Payment card liability and costs

eCrime

- Fraudulent instruction
- Funds transfer
- Telephone fraud.

Criminal reward coverage

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.

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.

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 live 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.

Real estate

Rogue employee

- An employee of a Real Estate Investment Trust (REIT) accessed the REIT's web-based HR system without authorization. The insured worked with panel counsel and a notification and call center vendor to notify approximately 1,500 individuals. Because Social Security numbers were viewed, the insured offered credit monitoring. A US Securities and Exchange Commission inquiry followed, but has since closed.

Hacking and malware

- A property management company that operates several spa hotels contacted Beazley when it believed one of its spa resort locations was infected with malware. Over the weekend, the BBR Services team coordinated with an external forensic team to be onsite that Monday to investigate. After an extensive investigation, it was discovered that the organization's central processing center (housed in a separate state) was infected. Based on available logs, the external forensic team was able to conclude that the malware had not accessed any personally identifiable information of patrons or employees. With counsel from an experienced privacy attorney, the insured was able to conclude that the incident was not a reportable breach.

Physical loss/non-electronic records

- A bank mailed mortgage documents to a couple closing on a home. The information included the couple's Social Security numbers as well as extensive financial history and information. The shipper lost the envelope, and the insured notified the couple and provided credit monitoring with BBR Services' assistance. When the courier company later discovered the envelope, but concluded that it may have been tampered with, the insured had already been notified by the bank and taken appropriate precautions.

Professional Services

CBSL330_US_11/17

Law firms

Hacking and malware

- A firm employee discovered malware on her laptop had sent emails to several contacts requesting the review of attached documents. BBR Services promptly assisted, recommending a forensic vendor to investigate the extent of the malware intrusion. The review of the email account determined that no personal information resided in her account during the time attackers had access to her email and no unauthorized access or acquisition of personal information occurred. Under US breach notice laws, the firm was under no legal obligation to notify any individuals.

Stolen portable device

- Thirty server hard drives and 10 desktop computers containing information on employees and clients were stolen from a law firm. Medical records of clients may also have been compromised, along with thousands of pages of other documents stored on the devices. BBR Services immediately assisted and connected the firm to expert privacy counsel and forensics. The insured ultimately notified 150 employees whose data was compromised and 25 other affected individuals.

Accounting firms

Hacking and malware

- When filing tax returns for clients, a CPA firm found that a cluster of clients had fraudulent returns already filed with the IRS. The firm contacted BBR Services, who put them in touch with panel privacy counsel. After discussing the issues with counsel, BBR Services connected the CPA firm with a panel forensic firm to conduct a review of certain laptops to determine if they were the source of the compromise. The forensic investigation revealed malware on the firm's systems that infiltrated client data. BBR Services coordinated the response, which included notification, call center services, and credit monitoring.
- After a CPA's email account was hacked, BBR Services connected him immediately with privacy counsel and computer forensic services to assist with his investigation. He learned that some of his client data, as well as clients' employee tax information, were potentially accessed in his email inbox. With assistance from a BBR notification and call center vendor, the insured notified 325 individuals and offered them credit monitoring.

Architects & engineers

Ransomware

- An engineering firm called BBR Services after a ransomware attack encrypted all of the firm's files – halting its business completely. The insured initially tried to handle the matter itself, but every time it restored files the virus kept encrypting them again. Desperate to isolate and eradicate the virus, the insured reached out to BBR Services, which coordinated a forensics team that was on-site in 12 hours deploying a network device which eventually isolated and stopped the virus from spreading.

Missing portable device

- The insured received notice that a construction field office was missing a hard drive that potentially contained a large number of sensitive records. Within 24 hours, the insured also was responding to a leak that resulted in several government demands pushing the insured to make notice to a large number of people. The insured called BBR Services, which immediately coordinated outside legal help and engaged a forensic firm to data mine the backup of the missing hard drive. During this process, the insured was able to show its due diligence immediately to the government body. The firm eventually used BBR's panel notification, call center, and credit monitoring provider to make a large notice in a very short timeframe.

beazley

Learn more:
www.beazley.com/bbr