Ransomware

We know data breaches. Since 2009 Beazley has managed over 7,000 data incidents across a variety of industries and causes, including ransomware. In 2016 and 2017, Beazley Breach Response (BBR) Services handled hundreds of ransomware incidents.

With thousands of ransomware attacks occurring on a daily basis, ransomware is a threat facing all organizations across all industries. Beazley's dedicated in-house team, BBR Services, provides timely ransomware assistance to BBR policyholders based on our repeated and extensive experience handling ransomware incidents.

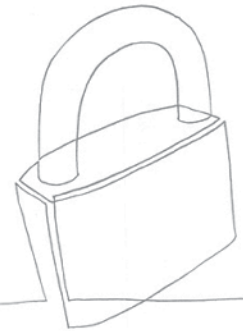
Cyber extortion and ransomware response services

If your organization is experiencing a ransomware attack, BBR Services assists by:

- Promptly consulting with your team to determine an appropriate response;
- Recommending and facilitating a fast connection with computer forensic services to determine if personally identifiable information or protected health information was compromised; and/or
- Facilitating introductions to service providers who can help you understand any data recovery options you may have, or if your organization decides to pay the ransom, who can secure Bitcoin, negotiate for you, and walk you through the decryption process.

BBR Services quickly coordinates services that help get your organization back to business.

- A physician practice discovered that its entire computer system, including its electronic medical record platform, had suddenly gone unresponsive. Multiple attempts to log on to the system failed. The practice then received an email from an unidentified individual, explaining that the sender had hacked their network, encrypted all information on the system, and would only decrypt the information for ransom payment. The doctors were ready to make the payment, but contacted BBR Services first. BBR Services immediately formulated a response strategy; engaging expert breach response counsel and coordinating with the FBI. The FBI and counsel explained that the attacker had a pattern of simply taking the ransom money, reneging on the agreement, and delivering additional malware onto the system. BBR Services coordinated the services the doctors needed in order to move forward and notify thousands of patients, federal regulators and the media about the incident.



Ransomware
continued

CBSL330_US_11/17

- A school district was hit with ransomware and two of its servers were completely encrypted. Critical documents were rendered inaccessible. BBR Services coordinated an engagement with forensics and legal counsel. Forensics was able to quickly identify the type of ransomware and determine its known capabilities. It was also able to find the decryption key for this particular strain of malware and use it to successfully restore all of the district's files.
- An engineering firm called BBR Services after a ransomware attack encrypted all of their files and stopped business completely. They initially tried to handle the matter themselves but every time they restored the virus kept encrypting files again. They call BBR Services and were desperate for any type of security help to try to isolate and eradicate the encryption virus. BBR Services coordinated a forensic team that quickly deployed a network device that eventually helped isolate and stop the virus from spreading.

BBR Services has developed a ransomware tip sheet, *Ransomware: Best Practices for Prevention and Response*, for BBR policyholders that explains the ransomware threat and the immediate steps companies facing this threat should take. This tip sheet can help your organization minimize the impact of a ransomware attack and speed up the recovery time following an attack.

You can download the tip sheet from our policyholder risk management website, beazleybreachsolutions.com, or you can email bbrservices@beazley.com to request a copy.

beazley

Learn more:
www.beazley.com/bbr