Beazley sees ransomware attacks quadruple in 2016, projects them to double again in 2017

NEW YORK, NY--(Marketwired - January 26, 2017) - Beazley, a leading provider of data breach response insurance, today released its *Beazley Breach Insights - January 2017* findings based on its response to client data breaches in 2016. The specialized Beazley Breach Response (BBR) Services unit saw ransomware attacks quadruple in 2016 and projects they will double again in 2017.

Organizations appear to be particularly vulnerable to attacks during IT system freezes, at the end of financial quarters and during busy shopping periods. Evolving ransomware variants enable hackers to methodically investigate a company's system, selectively lock the most critical files, and demand higher ransoms to get the most valuable files unencrypted.

Beazley's BBR Services division managed 1,943 data breaches on behalf of clients in 2016 compared to 1,247 breaches in 2015. Analysis of breaches handled by Beazley in 2016 revealed:

- **Ransomware keeps rising**
  Ransomware attacks were over four times higher in 2016 than in 2015. The ease and effectiveness of these attacks portend an even larger increase in 2017 with Beazley projecting these attacks to double again in 2017.
- **Unintended disclosure is a real problem**
  The proliferation of criminals looking to profit from confidential information has made formerly minor mistakes much more dangerous. Unintended disclosure, most often emails or faxes sent to the wrong recipient, increased to 32% of all breaches in 2016, up from 24% in 2015.
- **Financial institutions see more hacking attacks**
  Hacks and malware accounted for 40% of financial institution data breaches in 2016, up from 27% in 2015. Unintended disclosure -- mainly caused by misdirected emails -- was also up, rising to 28% of breaches in 2016 from 24% in 2015.
- **Higher education hacks are increasing**
  Hacks and malware accounted for nearly half of higher education data breaches in 2016 (45%), up from 35% of breaches in 2015. Unintended disclosures caused 28% of breaches in 2016, up from 22% in 2015.
- **Healthcare mixups drive breach exposures**
  Unintended disclosure -- misdirected faxes and emails or the improper release of discharge papers -- led to 40% of breaches in the healthcare industry in 2016, up from 30% in 2015. In a sign that the industry might be improving defenses, hacks and malware accounted for only 19% of breaches in 2016, down from 27% in 2015.

The Beazley BBR Services team offers clients cyber extortion and ransomware response assistance connecting clients with forensic services to determine if personally identifiable information or protected health information was compromised in the event of a ransomware attack. BBR Services also facilitates introductions to service providers to assist with data decryption, data restoration, or securing bitcoin if an organization decides to pay the ransom.

Katherine Keefe, global head of BBR Services, said: "The threat from ransomware is not only growing, but evolving to allow hackers to target vulnerable organizations and their most valuable data files and adjust ransom demands accordingly. The sustained increase in these threats in 2016 indicates that even more organizations will be attacked in 2017 and need to have incident response plans in place before they get a ransomware demand."

Read the Beazley Breach Insights - January 2017 report.

About Beazley Breach Response (BBR)

Beazley has helped clients handle more than 5,000 data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches. Beazley's BBR Services team coordinates the expert forensic, legal, notification and credit monitoring services that clients need to satisfy all legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.