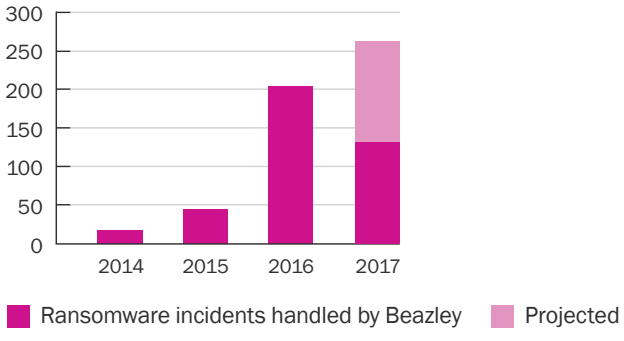
Ransomware attacks steal headlines, but accidental data breaches remain a major cause of loss

Ransomware attacks continued their rise in the first half of 2017, up by 50% over the first half of 2016.

Hacking and malware attacks (of which ransomware attacks form a growing part), continue to be the leading cause of breaches, accounting for 32% of the 1,330 incidents that Beazley Breach Response Services helped clients handle in the first half of the year.

Healthcare was the sector that experienced the highest increase in ransomware demands at 133%.

Ransomware incidents handled by Beazley



Source: BBR Services

However, accidental breaches caused by employee error or data breached while controlled by third party suppliers continue to be a major problem, accounting for 30% of breaches overall, only slightly behind the level of hacking and malware attacks. In the healthcare sector these accidental breaches represent, by a significant margin, the most common cause of loss at 42% of incidents.

This continuing high level of accidental data breaches suggests that organizations are still failing to put in place the robust measures needed to safeguard client data and confidentiality. Since 2014, the number of accidental breaches reported to Beazley's team has shown no sign of diminishing. As more stringent regulatory environments become the norm, this failure to act puts organizations at greater risk of regulatory sanctions and financial penalties.

The BBR Services unit worked with Beazley's insured clients to provide legal and forensics services in response to June's NotPetya ransomware attacks. The ability to respond quickly to ransomware attacks is especially critical for healthcare organizations due to the Office for Civil Rights (OCR) treating all ransomware attacks as a presumed breach.

CBSL441_US_07/17

2017 data breach trends

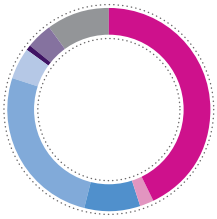
Schoolyard errors
Unintended disclosures caused 26% of breaches in 1H 2017 in the higher education sector. While slightly down on the 28% recorded in 1H 2016, this still represents a quarter of all breaches which could be mitigated through more effective controls and processes. Hacks and malware accounted for nearly half of higher education data breaches in the first six months of 2017 (43%), roughly even with the 45% of breaches caused by hacking in the same period in 2016. Of these, 41% were due to phishing.

Mistakes in healthcare
Unintended disclosure – such as misdirected faxes and emails or the improper release of discharge papers – continued to drive the majority of healthcare losses, leading to 42% of industry breaches in 1H 2017, equal to the proportion of these breaches in the industry in 1H 2016. Hacks and malware accounted for 18% of healthcare data breaches in 1H 2017, compared to 17% in 1H 2016.

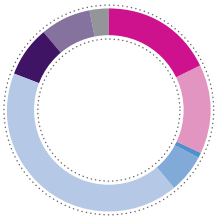
Unintended disclosures among financial services firms
Unintended disclosure – sending bank account details or personal information to the incorrect recipient – grew to 29% in 1H 2017 from 25% in 1H 2016, a level that has remained consistent since 2014. Hacks and malware were on a downward trend representing 37% of breaches in 1H 2017 compared to 46% of breaches in 1H 2016.

Professional services on the wrong track
At first glance, professional services firms appear to have greater internal controls in place with unintended breaches accounting for 14% of all incidents, well below the average for the period in question. However, the trend is tracking adversely, up from 9% in 1H 2016. Firms in the sector were not immune to hacking and malware attacks, with these incidents accounting for 44% of breaches in the time period compared to 53% in 1H 2016. Social engineering scams, including W2 fraud and requests for fraudulent wire transfers, were a large driver of attacks at the beginning of 2017.

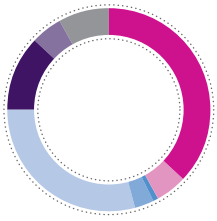
Higher education incidents, 1H 2017



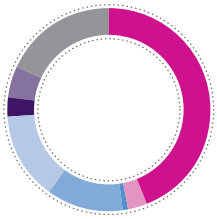
Healthcare incidents, 1H 2017



Financial services incidents, 1H 2017



Professional services incidents, 1H 2017



Four steps organizations can take to help protect their data

Perfect cyber security is impossible to attain, but there are steps organizations can take to protect their data. Here are four key steps organizations can take to minimize the risk:

- Deploy prevention and detection tools;
- Use threat intelligence services;
- Train managers and employees on cyber security, threat awareness and phishing; and
- Conduct risk assessments focused on identifying and protecting sensitive data.

About Beazley Breach Response (BBR)

Beazley has helped clients handle more than 6,000 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.

beazley

www.beazley.com/bbr