



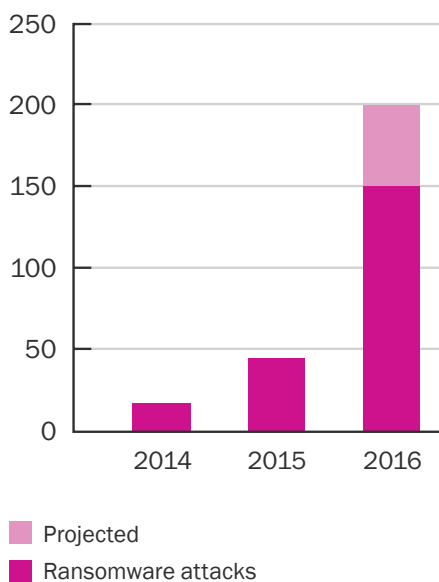
Ransomware attacks set to quadruple in 2016.

Ransomware attacks continued to increase rapidly during the first nine months of 2016. The trend was particularly pronounced in the financial services, retail and hospitality sectors. Ransom demands remain small, averaging just \$1,000.

New ransomware variants like Zepto, the increased availability of ransomware-as-a-service, and readily available toolkits make it easy for less sophisticated attackers to launch these types of attacks. Most organizations are infected because an employee clicks on a malicious attachment or a bad link in an email message.

During the first nine months of 2016, Beazley's BBR Services division managed 1,437 data breaches on behalf of clients, compared to 931 breaches during the same period last year.

Ransomware attacks: 2014 through end September 2016

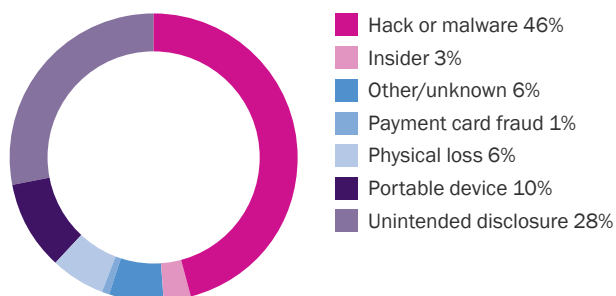


Source: BBR Services

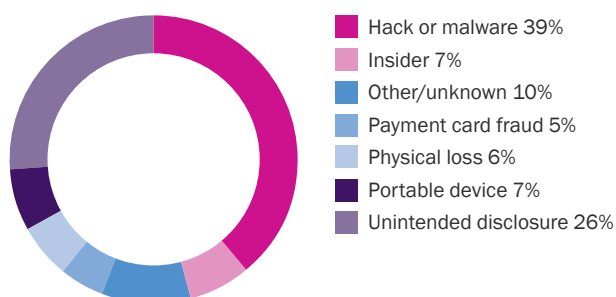
2016 data breach trends

- **Your money or your data** – Ransomware attacks are rising sharply, with more attacks in just July and August of 2016 (52) than Beazley handled in all of 2015 (43). Beazley projects it will respond to 400% more ransomware breaches in 2016 than it did last year.
- **Hacks are persistent** – The proportion of data breaches deriving from hacking and malware attacks in the first nine months of this year across all industries in Beazley's portfolio stood at 31%, in line with the percentage of such incidents observed in 2015 (32%).
- **Trying to break the bank** – Financial institutions are facing a higher proportion of breaches utilizing hacking and malware. Through Q3 of 2015, hacking and malware attacks accounted for 26% of the breaches Beazley handled for financial institutions; in the first nine months of 2016 that rose to 39%.
- **My homework got hacked** – Nearly half of 2016 data breaches at higher education institutions (46%) were caused by hacking or malware, up from 38% of industry breaches in the first nine months of 2015.
- **The doctor misplaced your file** - Within healthcare organizations, breaches caused by unintended disclosure represented 40% of all industry incidents in 2016 to date, a sharp rise from 28% in the first three quarters of 2015. This is connected to the large amount of information shared between organizations in this industry. 19% of healthcare breaches were caused by hacking or malware in 2016, down from 28% in 2015.
- **Next register, please** - The rate of hacking and malware in the retail industry remained high, accounting for 53% of all retail data breaches handled by BBR Services in the first nine months of 2016, compared to 51% in 2015.

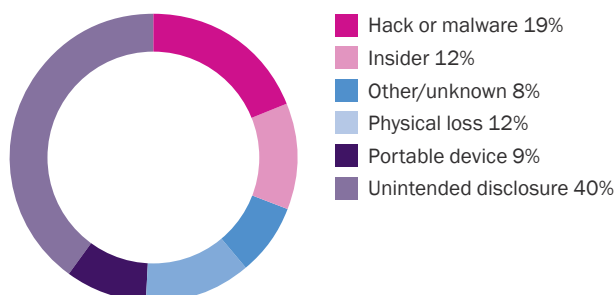
Higher Education Incidents, 2016



Financial Services Incidents, 2016



Healthcare Incidents, 2016



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 and threat awareness; and
- Conduct risk assessments focused on identifying and protecting sensitive data.

About Beazley Breach Response (BBR)

Beazley has helped clients handle more than 4,500 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.



www.beazley.com/bbr