Nine-fold rise in data breaches due to social engineering

Beazley's latest Breach Insights report reveals that while hacking and malware attacks prevail as the leading category of data breaches, social engineering attacks have risen nine-fold in 2017.

A social engineering attack occurs when a hacker uses deception to manipulate individuals into divulging confidential or personal information.

The two most prevalent types of incidents that we classify as under this heading are: fraudulent instruction incidents and W-2 scams.

Fraudulent instruction is a variant of business email compromise (BEC), in which a fraudster impersonates a trusted party, such as a company executive, a payment system vendor, or a participant in a real estate transaction. The fraudster then provides fraudulent payment instructions to divert a planned payment or to cause a fraudulent payment to be made.

Social engineering incidents rose from 1% in Q1-Q3 2016 to 9% of the 2,013 incidents managed by Beazley Breach Response (BBR) Services in Q1-Q3 2017. It is further confirmation that criminals are turning their attention to prey on human weaknesses in processes and controls rather than on technological vulnerabilities.

Over the course of 2017, Beazley's Breach Response (BBR) Services team has seen cybercriminals using social engineering more aggressively: 50% of social engineering breaches reported in the third quarter involved fraudulent instruction, up from 17% in the first quarter 2017. This increase in percentage from the first to the third quarter is attributable to the high number of W-2 email scams in the first quarter. Attackers took advantage of the tax season-related scam and then turned their efforts to fraudulent instruction.

Professional service firms had the highest percentage of social engineering breaches, followed by financial institutions and higher education institutions.

Hacking and malware remained the most prevalent cause of data breach at 34% of the total reported to Beazley in the first nine months of 2017. Hacking and malware includes cyber extortion which accounted for 30% of these. Incidents due to unintended disclosure were still a leading cause, despite having dipped slightly from 35% in Q1 2017 to 29% for the first nine months of 2017.

Social engineering can be quicker, easier and cheaper to implement for cybercriminals than stealing data and can be much more lucrative. As a leading data breach insurer, Beazley is concerned at the rapid development of this trend. We are urging our clients to implement tighter security and internal process controls, such as a requirement for dual authorization, and ensure that their employees are fully trained to spot potential attacks in order to reduce the chances of this happening.

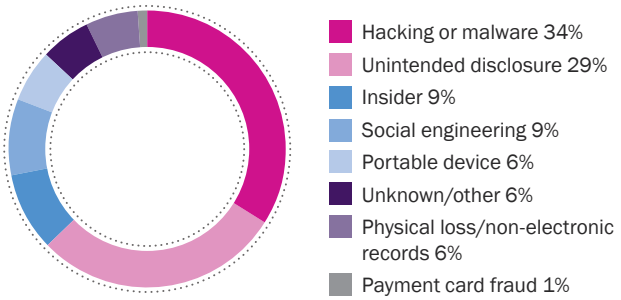
Healthcare – unintended disclosure unabated

At 41% of the total number of breaches reported to Beazley by organizations in the healthcare sector, the high level of unintended disclosure is unabated and remains more than double that of the second most frequent cause of loss, hacking or malware (19%). Beazley also noted an upturn in the number of data breaches caused by insiders, up from 12% of the total in 2016 to 15% in 2017.

Higher Education – mailbox vulnerabilities exposed

Phishing remains a prevalent cause of data breach for institutions in the higher education sector. (We classify this under hacking and malware.) Higher education incidents so far this year have involved one specific type of phishing scheme targeting employee direct deposit instructions. Attackers gain access to an employee's email inbox through phishing, determine the type of payroll/HR system that the institution uses, request a password reset for the employee's login to the system, and divert the electronic deposit of the employee's pay check. Many higher education institutions publish email contacts for faculty and staff on their websites, making them easier targets than organizations in other industries.

Causes of Data Breaches Reported, Q1-Q3 2017



Social engineering breaches by industry sector reported to Beazley, Q1-Q3 2017

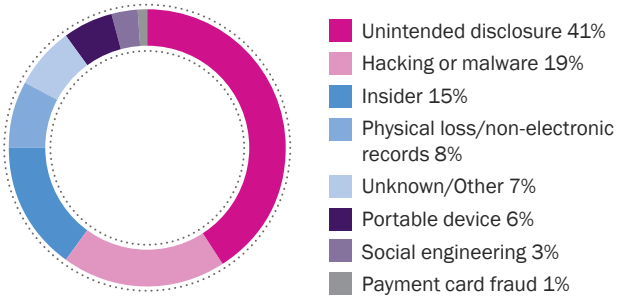
Professional service firms – 18%

Financial institutions – 9%

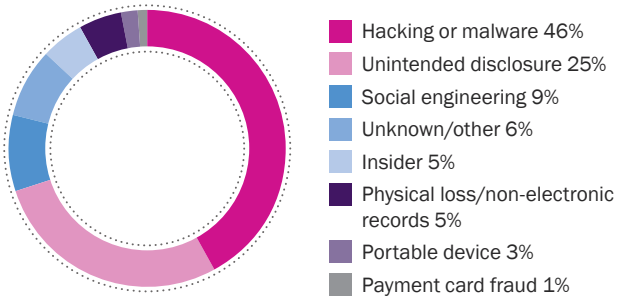
Higher education – 9%

Healthcare organizations – 3%

Healthcare Incidents, Q1-Q3 2017



Higher Education Incidents, Q1-Q3 2017



CBSL441_US_10/17

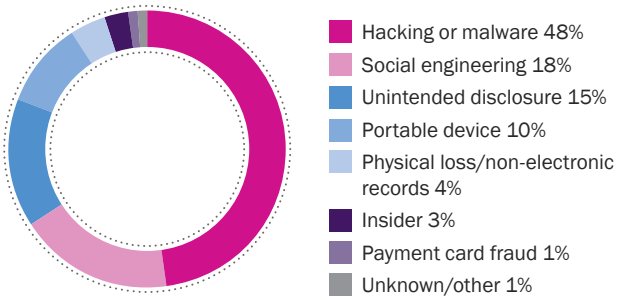
Professional Services – social engineering the fastest growing cause of breach

For professional services the highest percentage cause of breach in Q1-Q3 2017 was hacking and malware at 48%. However, social engineering has emerged as a worrying trend, accounting for 18% of all breaches reported to Beazley by firms operating in this sector, and almost double that recorded for financial institutions and higher education establishments.

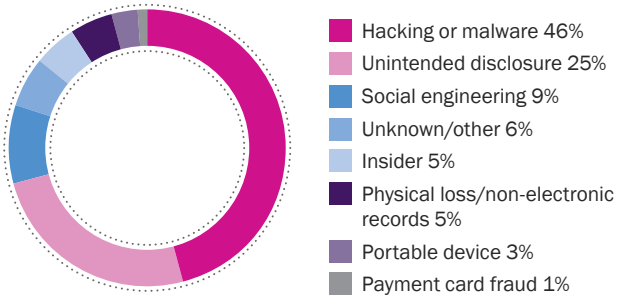
Financial Institutions – hacking and malware on the rise

Hacking and malware attacks as a proportion of the total number of data breaches reported to Beazley by financial institutions clients rose to 46% in the first nine months in 2017, up from 40% in the same period in 2016. Consistent with the overall findings of Beazley's Breach Insight report for the third quarter 2017, social engineering emerged as the fastest growing trend, representing 9% of all breaches.

Professional Services Incidents, Q1-Q3 2017



Financial Institutions Incidents, Q1-Q3 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 and threat awareness
- Conduct risk assessments focused on identifying and protecting sensitive data.

About Beazley Breach Response (BBR)

During the first nine months of 2017, Beazley Breach Response Services, Beazley's in-house team of breach response experts, managed 2,013 incidents on behalf of clients, compared to 1,943 incidents during the whole of 2016.

Beazley has helped clients handle more than 7,000 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.

To find out more about our services and how we can help your organization, visit www.beazley.com/bbr

beazley

www.beazley.com/bbr