Beazley sees new phishing threats emerge

Phishing scams aimed at accessing direct deposit funds have emerged as a new danger in 2017. Phishing scams aimed at accessing employee W-2 tax information were also a continuing threat, representing 9% of all breaches handled by Beazley in the first three months of 2017.

Ransomware attacks continued their rise in the first quarter of 2017, increasing by 35% over Q1 2016, after quadrupling in 2016.

During the first quarter of 2017, Beazley's BBR Services division managed 641 incidents on behalf of clients, compared to 462 incidents during the same period last year.

CBSL441_US_04/17

2017 data breach trends

Direct deposit deception
Beazley has seen an increase in hackers using phishing techniques to infiltrate employee email accounts and change their direct deposit account details. Once hackers have access to an employee's email, they request a password reset from the organization's payroll provider and change the employee's inbox forwarding rule to send all emails from the payroll provider to the target's junk mail. The hackers then change the employee's direct deposit bank account details to their own to steal funds. In addition, they may also access the employee's W2 information and file a fraudulent tax return.

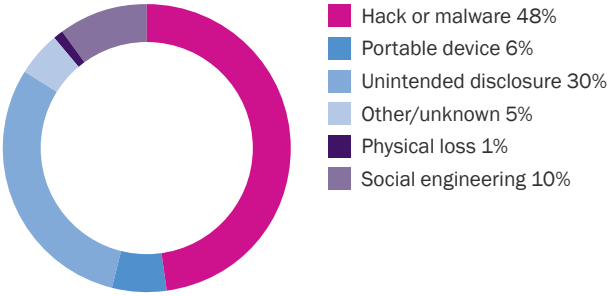
The majority of direct deposit phishing attempts occurred in the higher education sector where hacks and malware caused 48% of data breaches in Q1 2017, similar to the 50% of breaches they caused in Q1 2016.

Ransomware keeps increasing
Ransomware attacks continue to proliferate across industries and were 35% higher in Q1 2017 than in Q1 2016. Although the number of ransomware attacks continues to increase rapidly, Beazley's legal and forensic firms partners were able to retrieve seized client data without the client making ransom payments in the majority of incidents.

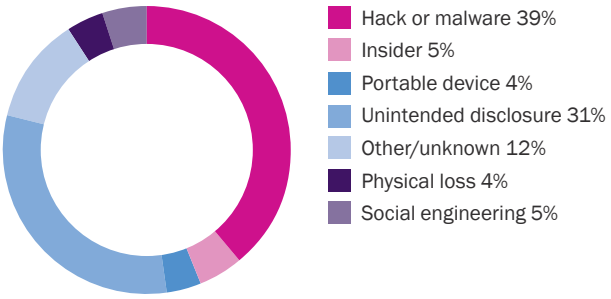
Hacked hospitals
Unintended disclosure – misdirected faxes and emails or the improper release of discharge papers – continued to be the largest single driver of healthcare losses, leading to 45% of industry breaches in Q1 2017 compared to 46% in Q1 2016. Insiders also persist as a threat in the healthcare industry; accounting for 12% of breaches in Q1 2017, up slightly from 10% in Q1 2016.

Breaking the bank
Hacks and malware continued to drive a large proportion of financial institution data breaches, representing 39% of breaches in Q1 2017, equal to the proportion of these breaches in the industry in Q1 2016. Unintended disclosure – sending bank account details or personal information to the incorrect recipient – is another leading cause of data breaches in this industry, representing 31% of breaches in Q1 2017, up from 26% in Q1 2016.

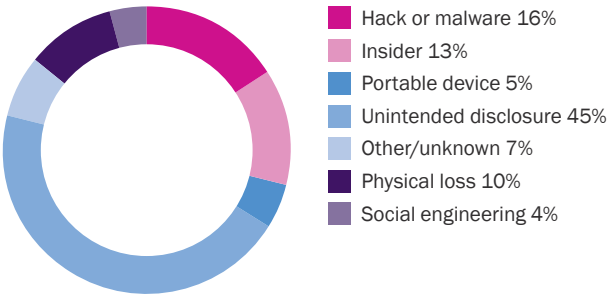
Higher Education Incidents, 2017



Financial Services Incidents, 2017



Healthcare Incidents, 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; and
- Conduct risk assessments focused on identifying and protecting sensitive data.

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.

beazley

www.beazley.com/bbr