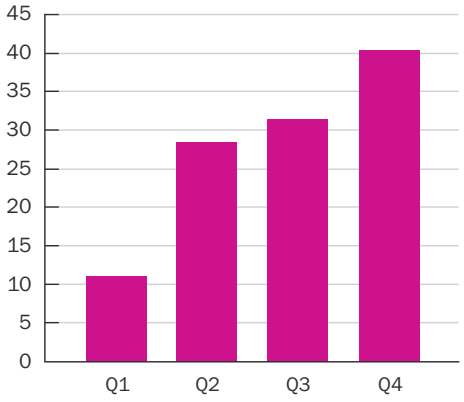
Fraudulent instruction emerges as significant new cyber threat

Claims data recorded by Beazley indicates that organizations are facing an increased threat to their operations from fraudulent instruction scams. Fraudulent instruction incidents reported to Beazley Breach Response Services (BBR Services) quadrupled in 2017, with policyholders incurring losses ranging from a few thousand dollars up to $3 million. With claims amounts in 2017 averaging $352,000, fraudulent instruction has rapidly become a significant financial threat to many organizations.

Cyber-criminals are using ever-more sophisticated methods to exploit human weaknesses in an organization's cyber-defences. Under fraudulent instruction scams, criminals use hacking and phishing techniques to accumulate information that allows them to send plausible-looking requests to transfer funds to bogus accounts. In addition to losing money, organizations may also have to conduct exhaustive systems analysis to ensure that individuals' personal and private data has not been compromised.

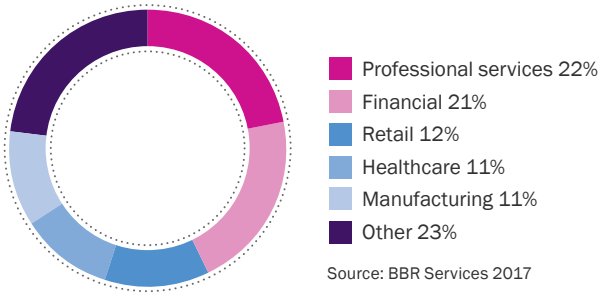
Fraudulent Instruction Incidents Reported to BBR Services, 2017



The top three industry sectors affected in 2017 were professional services (22% of the total reported to Beazley), financial services (21%) and retail (12%), but incidents are growing across all sectors, and in particular where single large transactions, such as real-estate purchases, are involved.

Katherine Keefe, global head of BBR Services commented, "Cyber-criminals are finding new ways of getting organizations to part with their hard-earned cash. In 2017 we saw fraudulent instruction emerge as a new trend which offers significant reward for the perpetrators in return for little effort, but brings potentially devastating financial consequences for the victim."

Fraudulent Instruction by Industry



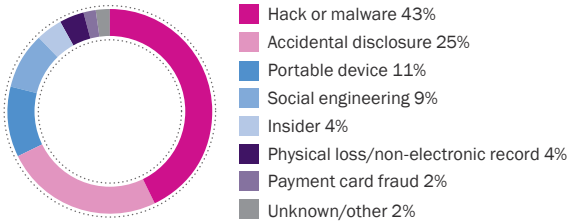
Source: BBR Services 2017

The main causes of data breach incidents reported to BBR Services in Q4 2017 remained hacking or malware (39% of the total reported to Beazley), accidental disclosure (21%) and social engineering (12%), which for the purposes of this report includes fraudulent instruction. To reflect the growth of fraudulent instruction we will create a separate category in our analysis below with effect from Q1 2018.

Breaches by industry

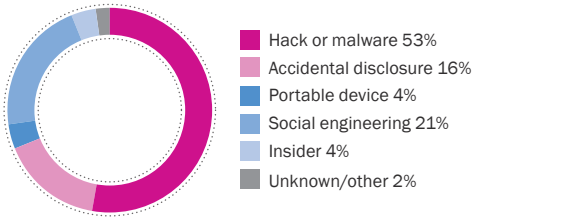
Higher education
Organizations in the higher education sector remained highly vulnerable to hacking and/or malware attacks in Q4 2017. In addition, the rates of accidental disclosure, at 25% and loss of portable device at 11% were above the Q4 2017 average reported to Beazley.

Higher Education Incidents, Q4 2017



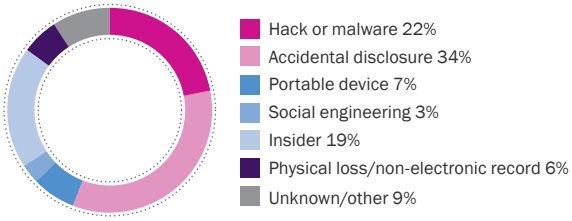
Financial services
Two worrying trends beset the financial services sector in Q4 2017. First, the number of breaches due to hacking and/or malware attacks rose sharply to 53% (Q1 39%). Second, social engineering scams quadrupled between Q1 and Q4.

Financial Services Incidents, Q4 2017



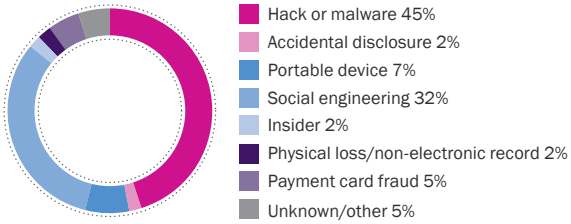
Healthcare
While still the highest cause of loss, accidental disclosure, a consistent cause of data breach in this sector, dipped from 45% in Q1 to 34% in Q4 2017, suggesting that more stringent processes and procedures may be bearing fruit. Between Q1 and Q4 2017, data breaches caused by hacking and/or malware attacks rose 50% among healthcare organizations to 22% of the total, making these the second-highest cause of healthcare data breaches.

Healthcare Incidents, Q4 2017



Professional services
Social engineering incidents doubled between Q1 and Q4 in the professional services sector. Services firms are targeted for similar reasons as financial services organizations, the cyber-criminal stands to gain significant lucrative rewards from successful scams.

Professional Services Incidents, Q4 2017



CBSL441_US_01/18

How fraudulent instruction works

After a successful phishing expedition or through the installation of a key-logger, a criminal can gain insight into company financial protocols related to wire transfers.

The criminal then uses a relationship that they have discovered through their phishing activities to provide fake payment instructions. The purported source of the payment instructions is often a trusted business partner.

Real estate transactions are frequent targets with the cyber-criminal exploiting the short timeframe for payment to take place. In a recent incident, the cyber criminal compromised a broker's email and sent revised wire transfer instructions, diverting the final payments.

Even with no access to earlier communications between the sender and recipient, a "spoofed" email can be created by checking social media for connections, roles or other supporting details.

One such attack came to light when a retail store received complaints from customers about non-delivery of goods for which they had paid by wire transfer. For the retailer however, there was no record of payment. It transpired that the customers had received new wire instructions from the criminals posing as the retailer.

Manufacturers are also vulnerable. In an incident reported to BBR Services, the email account of an employee in the accounting department of a manufacturer was compromised through phishing and the criminal emailed new wire payment instructions to some of the company's customers. Only after customers appeared to have missed payment did the manufacturer discover the account had been compromised.

The Beazley Breach Response Services team

Beazley has helped clients handle more than 7,500 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.

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

beazley

www.beazley.com/bbr