Hackers target smaller financial institutions

Hackers are training their sights increasingly on smaller financial institutions and their valuable client financial data. That does not mean that other businesses are no longer targets.

During the first half of 2016, Beazley Breach Response (BBR) Services managed 955 data breaches on behalf of clients, compared to 611 breaches during the same period last year. After healthcare, financial institutions, particularly those with annual revenues below $35 million, experienced the highest levels of breaches.

Within the financial institutions segment, hacking and malware attacks increased sharply as a proportion of total breaches as hackers went after their valuable financial data, increasingly targeting smaller and more vulnerable institutions. In 2015, hacking and malware accounted for 27% of the 128 financial insitution breaches handled by Beazley; in the first half of this year, that rose to 43% of 139 breaches handled.

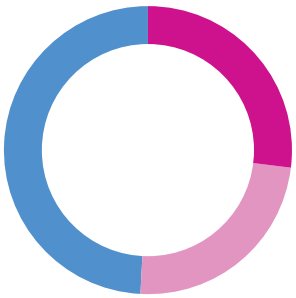
Banks and credit unions with less than $35 million in annual revenue accounted for 81% of hacking and malware breaches at financial institutions in 2016, a major increase over the 54% of incidents they represented in 2015. Hackers are increasingly targeting smaller financial institutions with less robust data security systems and personnel than larger banks.

2016 data breach trends

Across all industries in Beazley's portfolio, the proportion of data breaches deriving from hacking and malware attacks in the first six months of this year stood at 31%, in line with the proportion of incidents observed in 2015 (32%).

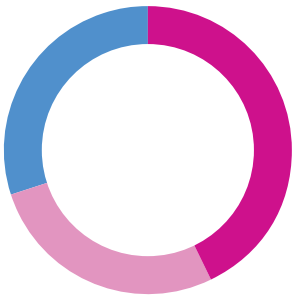
- Higher education institutions continued to see a high proportion of breaches due to hacking or malware with these accounting for 46% of breaches in the first half of 2015, up from 35% in 2015.
- Within healthcare organizations, breaches caused by unintended disclosure represented 42% of all industry incidents in 2016 to date, a sharp rise from 30% in 2015. This is driven by the large amount of information shared between organizations in the industry. 18% of healthcare breaches were caused by hacking or malware in 2016, down from 27% in 2015.
- Retail industry breaches caused by hacking and malware remained high, accounting for 49% of all retail data breaches in 2016 compared to 55% in 2015.
- Ransomware attacks continue to increase, with twice as many attacks in the first six months of 2016 (86) than Beazley handled in all of 2015 (43).

Financial institutions – Leading breach causes, 2015



Hacking or malware, 27%
Unintended disclosure, 24%
Other, 49%

Financial institutions – Leading breach causes, first half 2016



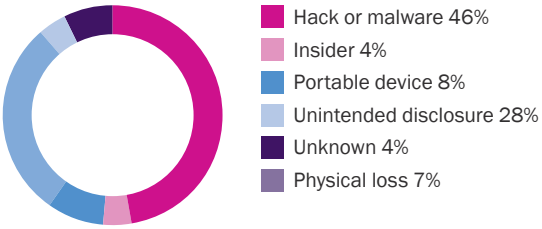
Hacking or malware, 43%
Unintended disclosure, 27%
Other, 30%

CBSL441_US_07/16

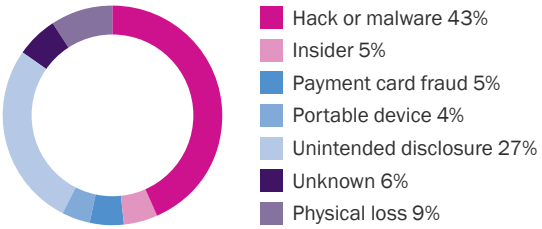
Smaller banks and credit unions are a growing target for hackers

The fastest growing segments being targeted within financial institutions are small banks and credit unions. Smaller financial institutions hold valuable personal information and many times do not have the same cyber security defenses in place to ward off hackers as their larger counterparts, making them an attractive target for hackers.

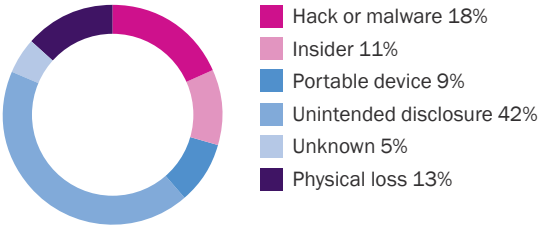
Higher Education Incidents, 2016 (Total: 108)



Financial Services Incidents, 2016 (Total: 139)



Healthcare Incidents, 2016 (Total: 533)



Source: BBR Services

Perfect cyber security is difficult to attain, but there are steps organizations can take to protect their data. Here are four key steps financial institutions 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.

Hacking examples in financial services

Phishing incident
A financial firm's systems were compromised due to a spear-phishing scheme that resulted in a fraudulent wire transfer and potential exfiltration of emails with customer personally identifiable information (PII). BBR Services recommended forensics and privacy counsel, and they concluded, after an extensive manual review of data, that the insured was legally obligated to notify approximately 3,000 individuals.

Malware incident type
A bank experienced a sophisticated malware attack, where hackers were in the insured's system for at least six months. The hackers set up fake accounts and money was withdrawn from the bank from those fake accounts. The forensic investigation was extremely expensive due to the type of malware. With BBR Services coordination, the bank notified and provided credit monitoring to nearly 30,000 individuals whose credit card numbers, social security numbers and driver's license numbers may have been exposed.

Vendor hacking incident
A financial services firm reported that the passwords for a web based dealer portal (which is licensed from a third party vendor) were compromised. Four dealer accounts were hacked and the routing and account numbers were transposed. This caused the firm to issue unauthorized deposits to dealers who did not actually request them. BBR Services connected the firm with panel privacy counsel and a forensic firm. After an investigation, counsel determined that the firm was required to notify approximately 600 individuals. BBR services coordinated the notification and call center services and helped the firm order credit monitoring codes for affected individuals.

About Beazley Breach Response (BBR)

Beazley has helped clients handle more than 4,000 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