Cyber Risks in the Financial Institutions Industry

The financial institutions industry inherently holds a robust amount of financial data and conducts many types of financial transactions, making it a prime target for bad actors. Consumers and businesses alike expect seamless and instantaneous transactions, which has led to several advances in technology, thus increasing the exposure to cyber risk.

That is why the industry faces steep regulations, including the Gramm-Leach-Bliley Act (GLBA) and the recent New York Department of Financial Services (NYDFS) cyber security regulations, both of which place stringent compliance and reporting requirements on all financial institutions. Although financial institutions are one of the most vigilant and prepared types of insured entities, the **Chubb Cyber Index**[SM] shows that the median cost of incident response services (e.g., call center, forensic services, notification, crisis response, etc.) for these organizations has climbed to nearly $1,636,653 during the past three years. This is nearly double the $827,623 median cost from 2009-2018.

Fast Facts

60% of incidents reported to Chubb in the Financial Institutions industry were caused by someone outside the organization

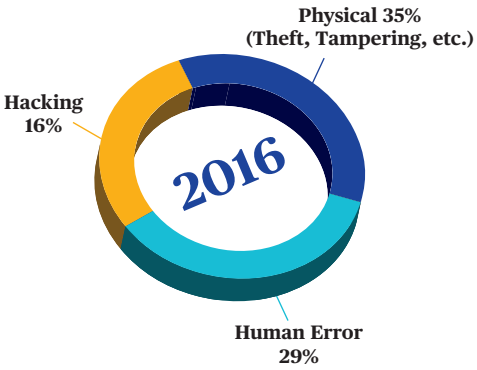
These external actions compromised individuals 38% of the time

and servers 33% of the time

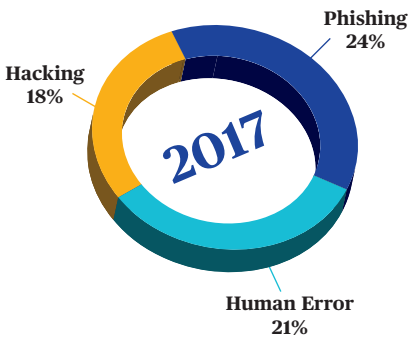
*2018 data from the Chubb Cyber Index[SM]

Despite the regulations and vigilant nature of the industry, the cyber risk landscape continues to evolve and change. Thankfully, so does the data on the **Chubb Cyber Index**[SM]. Knowledge of the latest risks and threats is one of the most important tools in your cyber defense arsenal. Regularly review the **Chubb Cyber Index**[SM] (www.chubb.com/cyber) to learn the latest cyber threats, and receive real-time access to Chubb's proprietary cyber incident data.

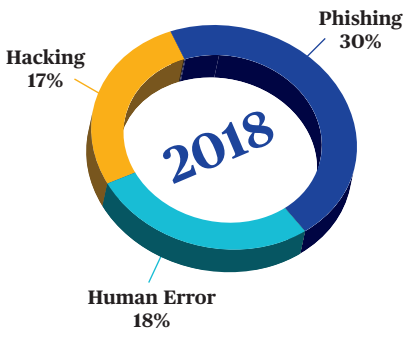
2016 Top Actions for Financial Institutions:



2017 Top Risks for Financial Institutions:



2018 Top Risks for Financial Institutions:



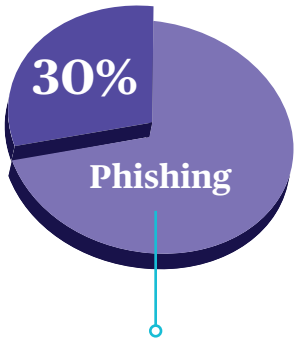
Services to Help Mitigate Cyber Risk:

Employee Education

Strong Password Hygiene

Vendor Management

Phishing Attack Nets Personal Data and Costs Millions



Accounted for **30%** of Cyber Claims Reported by Financial Institutions to Chubb in 2018.

The Claim

A midsize financial services company became the victim of a mass phishing attack after some of its employees clicked on a malicious link contained in an email. Once the malicious link was opened, bad actors were able to obtain system credentials, giving them access to approximately 100 email accounts. After the initial compromise, the bad actors set a forwarding rule on the compromised email accounts, which sent any new emails to an unauthorized email address. Many of the compromised email accounts contained the names and social security numbers of the company's clients. Additionally, the bad actors were able to access the company's other systems to make several fraudulent wire transfers. It was eventually determined that approximately 200,000 individuals' personally identifiable information was compromised by the phishing attack, thus triggering notification and two-year credit monitoring requirements for those affected individuals.

The Resolution

An incident response coach and a forensic firm that frequently handles these types of phishing scams were retained. Utilizing specialized tools to analyze which email accounts were compromised, the forensic firm concluded that several million documents needed to be reviewed to determine the nature and scope of the affected population. Chubb covered approximately $3.5M in first-party expenses: $2M for the forensic firm, $1M for the incident response coach, and $500,000 for credit monitoring and call center fees.

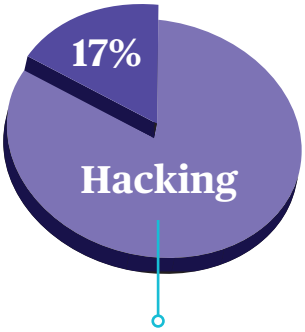
Ryuk Ransomware Scam Demands Bitcoin Payoff

The Claim

A financial services company was the victim of a highly targeted and planned Ryuk ransomware attack. Ryuk is a virulent form of ransomware that is characterized by large ransom demands. In this particular attack, the ransom demand was for more than $100,000 in Bitcoin, which the company refused to pay. This attack affected the company's entire network, rendering the company's data inaccessible. While the company had adequate backups of its system, it is still unclear as to whether full restoration is possible.

The Resolution

An incident response coach and a forensic firm from Chubb's recommended incident response team were retained, and are still working to determine if protected information was impacted in a manner that would trigger notification obligations under applicable data privacy laws. First-party expenses are still being incurred.



Accounted for **17%** of Cyber Claims Reported by Financial Institutions to Chubb in 2018.

SOURCE: The Chubb Cyber Index℠ (March 2019)

Chubb. Insured.℠