



## 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<sup>SM</sup>** 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.

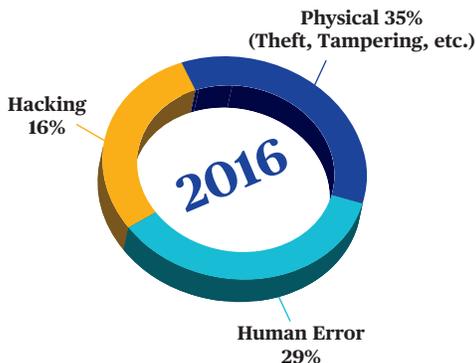
### Fast Facts



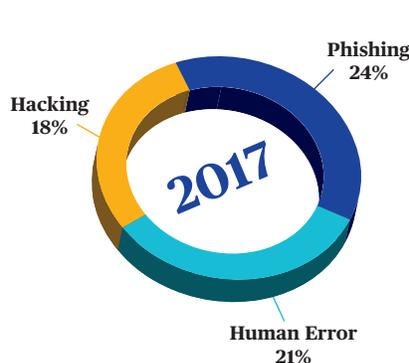
\*2018 data from the Chubb Cyber Index<sup>SM</sup>

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<sup>SM</sup>**. 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<sup>SM</sup>** ([www.chubb.com/cyber](http://www.chubb.com/cyber)) to learn the latest cyber threats, and receive real-time access to Chubb's proprietary cyber incident data.

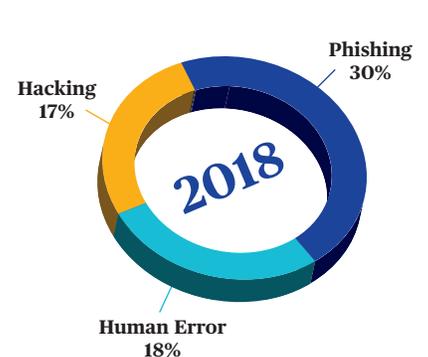
2016 Top Actions for Financial Institutions:



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

### 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.



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

### 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.

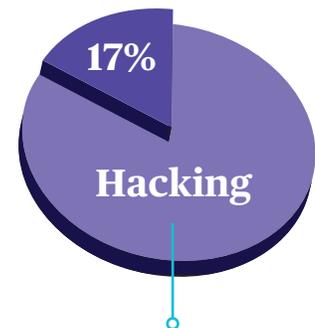
## Ryuk Ransomware Scam Demands Bitcoin Payoff

### 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<sup>SM</sup> (March 2019)

The scenarios described here are hypothetical and are offered solely to illustrate the types of situations that may result in cyber incidents and/or claims. These scenarios are not based on actual claims and should not be compared to actual claims. The precise coverage afforded by any insurer is subject to the terms and conditions of the policies as issued. Products may not be available in all locations, and remain subject to Chubb's underwriting criteria. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.

Chubb has no obligation to provide any cyber services for loss mitigation or incident response. The policyholder is under no obligation to contract for services with any of the Chubb pre-approved loss mitigation or incident response service providers. The selection of a particular pre-approved loss mitigation or incident response service provider is the independent choice of the policyholder. Chubb is not a party to any agreement entered into between any loss mitigation or incident response service provider and the policyholder. Loss mitigation and incident response service providers are independent contractors, and not agents of Chubb. Chubb assumes no liability arising out of any services rendered by a loss mitigation or incident response service provider, and Chubb does not endorse the service providers or their respective services. Before a policyholder engages with any loss mitigation or incident response service provider, the policyholder should conduct its own due diligence to ensure the company and its services meet the policyholder's needs.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at [www.chubb.com](http://www.chubb.com). In the United States, insurance is provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. All products may not be available in all states. This communication contains product summaries only. Coverage is subject to the language of the policies as actually issued. Surplus lines insurance is sold only through licensed surplus lines producers. Chubb Limited, the parent company of Chubb, is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index.

**Chubb. Insured.™**