Claims

COVERING THE BUSINESS OF LOSS

October 2018

Volume 66 . Number 10

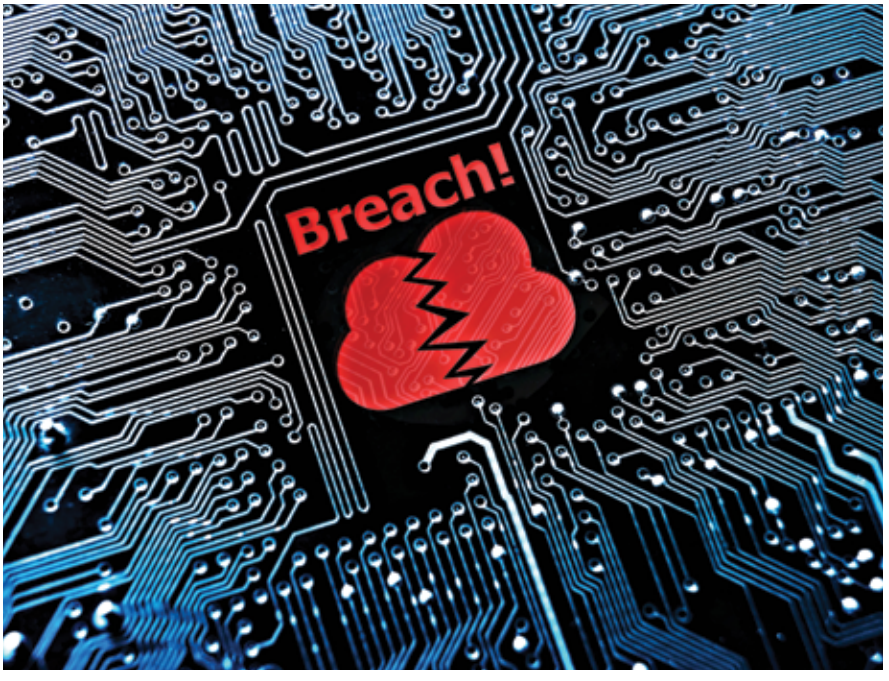
PropertyCasualty360.com

An ALM Publication

Reprinted with permission from the October 2018 issue of *Claims* magazine

The National Underwriter Company

Three Keys to Handling Cyber Claims



Recently, Ginni Rometty, president and CEO of IBM stated, "Cyber-crime is the greatest threat to every profession, every industry, and every company in the world."

For those in the insurance industry, that statement further validated the seriousness of cyber-crimes and underscored the need for insurance products and claims professionals to evolve and stay ahead of emerging cyber threats.

In 2000, a policy addressed cyber liability and business interruption claims. Since then, according to the Insurance Information Institute, more than 60 carriers offered stand-alone policies in a market encompassing gross premiums written at $3.25 billion in 2016. Carriers have also added coverage to package policies to address many of the needs.

Since as early as the 1700s, court decisions, regulations, opinions and training methods have refined the way the industry responds to losses. However, customer expectations and needs in today's digital world will not allow the passing of another 250 years to refine the process around handling cyber-related claims. By the end of 2019, Cybersecurity Ventures predicts there will be a ransomware attack on businesses every 14 seconds.

Cyber-related crimes

Claims handling expertise is at a premium because assessing and calculating damages in a cyber breach claim can be complex. To help customers, claims handlers need to focus on three areas: Understand the complexities of the particular attack waged and the technology behind it; determine whether coverage is available under the applicable policy; and identify the claims handling needs associated with the coverages.

There are multiple forms of cyberattacks. Carriers often work with cyber consultants to conduct a detailed investigation and forensic analysis. Claims professionals should know the difference between a phishing attack, data compromise, wire fraud, password attack or other cyber crime to identify the appropriate data rescue procedures.

Cyber claims adjusters should be experts in understanding the cyber policy, its application to both the first-and-third party, and how a customer's other coverages come into play. Identity theft coverage, data compromise coverage, cyber extortion, data compromise liability, computer and funds transfer fraud coverage, network security liability and reputation coverage are just the start of the coverages claims professionals need to understand when handling cyberattacks.

Claims professionals also need to pay attention to the emotional impact associated with cybercrimes. Similar to the victim of a physical attack, a cyber attack can have the same emotional effects on the aggrieved party. These crimes involve attacks on personal information, potential significant financial impact and potential harm to reputations. Knowing the technology, the coverage of the policies and the appropriate experts to work with can help alleviate some of the emotional stress related to a claim.

Cybersecurity Ventures predicts that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. In the United States, a Forbes article states the average data breach cost for businesses is $7.91 million. If the problem is not going away, focusing on understanding coverages, prevention and recovery is more important than ever.

Donald Meier, CPCU, (donaldmeier@westfieldgrp.com) is the property complex claims leader for Westfield Insurance.