BEST'S NEWS & RESEARCH SERVICE

BestWire - June 08, 2021 11:27 AM (EDT)

CYBER LIABILITY

Colonial Pipeline Ransomware Attack Could Signal Tough Road for Cyber Writers

By Caroline Saucer

OLDWICK, N.J. //BestWire// - The ransomware attack on the Colonial Pipeline caused real-world impact when the 5,000-mile U.S. fuel pipeline was shut down for six days. Now cyber insurers and observers are questioning how to respond to a world in which ransomware attacks are increasingly sophisticated, faster and more expensive.

Joshua Motta

It highlighted the real concern cyber experts have had that an attack could cause significant destruction to critical infrastructure and hurt the U.S. economy and way of life, said Jake Olcott, vice president of the security ratings firm BitSight.

But the basic elements of the attack — that cyber criminals took advantage of a vulnerability they found in a company's computer system — was something experts in cyber insurance have seen over and over, according to Joshua Motta, chief executive officer and co-founder of Coalition, one of the largest providers of cyber insurance in the United States.

The immediate response among insurers is to improve underwriting, raise prices and reduce their coverage, Motta said.

The attacks are getting more complex and widespread, and it's expected companies will be investing more in their information technology and security systems and on cyber insurance, said Fred Eslami, associate director who leads the cyber insurance initiative at AM Best.

With the cyberrisk hazard environment — ransomware, business interruption and aggregation — worsening significantly, prospects for the U.S. cyber insurance market are grim, according to a new Best's Special Report. The loss ratio for cyber insurance rose dramatically in 2020, to 67.8%, from 44.8% in 2019. However, the increase was not limited to just a few insurers — the loss ratio rose for 15 of the 20 largest cyber insurers, it found. Hackers are becoming more sophisticated in their attacks and moving toward larger targets.

Cyber insurance is now a primary component of a corporation's risk management and insurance purchasing decisions. Consequently, according to the report, insurers urgently need to reassess all aspects of their cyberrisk, including their appetite, risk controls, modeling, stress testing and pricing, to remain a viable long-term partner dealing with cyberrisk.

One of the largest and most intricate cyberattacks was discovered in December and led to an estimated $90 million in insured losses, according to BitSight. Russian cyber criminals targeted the utility software SolarWinds and eventually gained access to the systems of thousands of their customers, even getting their hands on emails from the United States Commerce, Justice and Treasury departments.

Copyright © 2021 A.M. Best Company, Inc. and/or its affiliates. ALL RIGHTS RESERVED. No part of this report or document may be distributed in any electronic form or by any means, or stored in a database or retrieval system, without the prior written permission of AM Best. While the content was obtained from sources believed to be reliable, its accuracy is not guaranteed. For additional details, refer to our *Terms of Use* available at AM Best website: www.ambest.com/terms.

Colonial Pipeline Ransomware Attack Could Signal Tough Road for Cyber Writers
(continued)

Another 2017 Russian military cyberattack on Ukraine that used the NotPetya virus resulted in $3 billion in insured losses and was declared a cyber catastrophe. Cyber catastrophes are events that lead to an economic loss of greater than $200 million, Olcott said.

Outside of the major headlines, thousands of smaller cyber and ransomware attacks happen on a regular basis to companies from all sectors, including insurers. CNA Financial Corp. recently revealed it had been hit with a sophisticated ransomware attack that caused the company to disconnect its systems and take action to contain it. Axa SA also reported it experienced a ransomware attack in Asia.

In 2020, there were nearly 2,400 ransomware attacks against U.S.-based governments, schools and health care facilities, according to a 2021 report from the Ransomware Task Force. Risk adviser Marsh has said more than half of organizations have been victims of ransomware attacks. American International Group, which offers cyber insurance, said on its website that global ransomware damages are expected to cost $20 billion in 2021.

The Ransomware Task Force reported Coalition saw the frequency of ransomware attacks among its policyholders rise 260% during the first half of 2020 and the average ransomware demand go up 47%.

In the case of Colonial Pipeline, the company's chief executive officer told the Wall Street Journal the company paid the cybercriminal group DarkSide $4.4 million within hours of finding out it had been hit with. It's a lot of money but not uncommon or shockingly large, said Michael Phillips, chief claims officer of managing general agent Resilience Insurance, who co-chaired the Ransomware Task Force.

"I'm certain that hundreds of ransoms in similar amounts are paid every year," he said.

The Best's Special Report noted hackers' motives also appear to be changing as well, from stealing identities (third-party claims) to shutting down systems for ransom (first-party claims). Total claims rose 18% in 2020, owing strictly to first-party ransomware claims, which were up 35% in 2020 and now account for 75% of cyber claims.

Keeping up

As frequency and severity rise, a major challenge for cyber insurers is the short-tail nature of the events, Phillips said.

Ransomware attacks can potentially lead to a large loss within days or weeks of writing a policy. "It's a bit like writing a property insurance policy for a building that gets knocked down the next day," he said.

Growth in premiums hasn't been able to keep up with claims, according to a May 11 Best's Commentary. Premium increases between 2017 and 2020 averaged 19%, but claims grew 38%.

Prices are going up dynamically. As soon as premiums seem to hit what appears to be their highest point, they go even higher, said Samantha Levine, senior vice president of CAC Specialty's professional and

Copyright © 2021 A.M. Best Company, Inc. and/or its affiliates. ALL RIGHTS RESERVED. No part of this report or document may be distributed in any electronic form or by any means, or stored in a database or retrieval system, without the prior written permission of AM Best. While the content was obtained from sources believed to be reliable, its accuracy is not guaranteed. For additional details, refer to our *Terms of Use* available at AM Best website: *www.ambest.com/terms*.

Colonial Pipeline Ransomware Attack Could Signal Tough Road for Cyber Writers
(continued)

cyber solutions.

"We're seeing, at this point, 100% increases in premium as the best options with double retentions," she said. Earlier in the year, the increases were in the 30% to 40% range. The hikes appear to be driven by continued ransomware attacks, which have been happening on a regular basis but haven't been reported in the media.

"The risk is continuing and there's no end in sight from an insurer's perspective," Levine said. "The right-sizing of the book is happening at a much quicker pace."

Insurers are also turning to sublimits in their ransomware coverages. Typically, cyber insurers offer coverage of up to $10 million in a single policy, which includes extortion. Very large companies that need more coverage can buy additional towers into the hundreds of millions of dollars if they need it. If they exhaust their primary coverage, the additional insurance kicks in.

However, that typical aggregate limit of $10 million has been cut by some insurers to $5 million, Levine said.

And if companies don't have the proper cybersecurity controls in place, the insurer may sublimit all coverage arising out of a ransomware event, including extortion, business interruption and first party notification. Insurers have added supplements to their application process that's pages long with multiple questions about cybersecurity, Levine said.

That is, if ransomware is included in the policy at all. In early May, Axa SA announced its French unit would suspend ransomware crime reimbursements (BestWire, May 10, 2021).

Demand Spurs Underwriting

Demand for cyber insurance, which had been high even before the Colonial Pipeline attack, continues to explode. "We're seeing a large increase in people now wanting to purchase cyber insurance who might have been nonbuyers previously," Levine said.

But buyers are facing a market that's cautious. "We're reaching a place where the supply of the available cyber insurance is constrained," Phillips said. "It's harder to match buyers and sellers to make sure companies have as much insurance as they want."

Phillips predicted the industry will undergo a radical transformation in the way energy and infrastructure firms are underwritten.

Historically, cyber underwriters have focused on information technologies and private information, developing expertise around privacy and office networks. When Target and Home Depot experienced payment card data breaches, millions of dollars were spent in the insurance industry to address the breaches and indemnify the firms. As a result, payment card industry standards were developed and underwriters devel-

Copyright © 2021 A.M. Best Company, Inc. and/or its affiliates. ALL RIGHTS RESERVED. No part of this report or document may be distributed in any electronic form or by any means, or stored in a database or retrieval system, without the prior written permission of AM Best. While the content was obtained from sources believed to be reliable, its accuracy is not guaranteed. For additional details, refer to our *Terms of Use* available at AM Best website: *www.ambest.com/terms*.

Colonial Pipeline Ransomware Attack Could Signal Tough Road for Cyber Writers
(continued)

oped expertise in those standards, Phillips said. Payment card data breaches are no longer an economic crisis.

He sees a similar evolution coming in regard to ransomware, with cyber insurers aggressively pursuing the appropriate level of expertise around infrastructural network and industrial control systems.

Relentless Threat

Although ransomware first appeared on the radar of security professionals and the insurance industry around 2016, it began taking on a new form in 2020 with more frequency and severity, said Motta.

It's happening in part because of the evolution of the cryptocurrency ecosystem. Cryptocurrency has allowed threat actors to move money more quickly, launder it and hide it, according Phillips.

It has resulted in a larger focus on standalone cyber policies, which were up 28% in 2020, and have seen a higher rate of growth compared with packaged policies, according to the Best's Special Report.

In a standalone cyber insurance policy, ransomware events typically trigger several coverages, including legal counsel; technical or forensic expertise to figure out how the hackers got access, what they took, and how to secure the systems again; data recovery and restoration; business interruption losses; and extortion coverage when a company decides it has no choice but to pay the ransom.

In many cases, it's legal in the United States to pay a ransom. However, it's prohibited if the hackers face sanctions from the Department of Treasury.

Often, insurers require their insureds use experts to help negotiate the ransom, assist in the cryptocurrency payment and help get the company back up and running. A small industry of firms that specialize in ransomware expertise has cropped up to negotiate with threat actors in a way that's compliant with law enforcement, Phillips said.

It might sound as if paying the ransom is part of the strategy of dealing with ransomware, but that's not true, according to Phillips.

"Cyber insurance brings to bear all of the types of expertise that can help a victim figure out what the options are and help determine the best option that is available to help them recover," he said. Ransom is paid when there's no other choice because of harm to the company, customers or employees.

Some have claimed that simply having ransomware coverage makes a company a target for an attack. Phillips and Levine dispute that claim. Bad actors "operate by trying to find vulnerabilities that they know how to exploit," Phillips said. "They're not just looking to scale the wall of a well-secured company because there might be insurance on the other side. They're looking for holes in the wall."

In many instances, hackers don't know what kind of company they're hacking into. But once they've

Copyright © 2021 A.M. Best Company, Inc. and/or its affiliates. ALL RIGHTS RESERVED. No part of this report or document may be distributed in any electronic form or by any means, or stored in a database or retrieval system, without the prior written permission of AM Best. While the content was obtained from sources believed to be reliable, its accuracy is not guaranteed. For additional details, refer to our *Terms of Use* available at AM Best website: *www.ambest.com/terms*.

Colonial Pipeline Ransomware Attack Could Signal Tough Road for Cyber Writers
(continued)

gained access, they may realize there's a cyber insurance policy. When they can see how much coverage the company has for extortion, they ask for more, Levine said.

As insurers find ways to fight ransomware, there's still more to learn. Phillips estimated that globally, perhaps only 15% of organizations have cyber insurance. That means insurers probably only see a very small portion of the total number of attacks that happen every year. Not knowing the full picture can make it harder to find an effective way to confront the problem.

(By Marie Suszynski, BestWeek correspondent)

Copyright © 2021 A.M. Best Company, Inc. and/or its affiliates. ALL RIGHTS RESERVED. No part of this report or document may be distributed in any electronic form or by any means, or stored in a database or retrieval system, without the prior written permission of AM Best. While the content was obtained from sources believed to be reliable, its accuracy is not guaranteed. For additional details, refer to our *Terms of Use* available at AM Best website: *www.ambest.com/terms*.