Plugging the Cyber Gap

Marrying property and cyber coverage seamlessly is an area of increased focus for risk managers and underwriters.

By Alex Wright

Bolting cyber coverage onto property coverage is a challenging task for manufacturers and others.

Manufacturing and logistics companies are living in constant fear of the next big cyber event. Advancements in smart technology and interconnectivity in the manufacturing and supply chain process only heighten cyber risk.

This has had the unintended consequence of leaving companies more vulnerable to cyber attacks than ever, as evidenced by the recent spate of NotPetya and WannaCry attacks that devastated many businesses last year. Once hackers get hold of the relevant codes, they can shut down entire manufacturing processes and supply chains, causing untold damage and costing companies billions in lost revenue.

As a result, demand for cyber coverage has spiked over the last year. However, given the relatively new nature of cyber as a risk, there's less historical data available, making coverage harder to find.

Added to that, as an admitted risk, property coverage is regulated on a state-by-state basis. But because cyber risk is non-admitted, bolting it on to an existing property program, particularly for a company operating in multiple states, can be problematic because of the different way the two types of cover are regulated.

An even deeper-lying issue: Many companies don't understand what coverage they have and whether they will be covered for a cyber event that causes property damage or business interruption. This was tested by last year's NotPetya cyber attack on Merck & Co, which disrupted production of its medicines and vaccines on a mass scale. The company has yet to quantify its total losses.

"We have seen a definite increase in the inclusion of non-physical business interruption coverage within manufacturers' property policies," said Tracie Grella, global head of cyber insurance, AIG.

"Since property policies provide coverage for business interruption caused by physical loss, it is only logical to want to extend coverage within the property policy to include business interruption caused by a cyber attack, rather than by having a standalone cyber product."

SYSTEM FAILURE

Emy Donovan, global head of cyber and tech PI, Allianz Global Corporate & Specialty, said cyber threat increased as a result of manufacturing companies connecting more of their processes to the internet. Added to that, there has been a move toward smarter processes, which, when they go wrong, can leave the company exposed to even wider business interruption (BI) problems, she said.

> *"Following the surge in ransomware and destructive malware that we witnessed in 2017, the awareness of cyber risk among more traditional industries has risen."*
>
> ***— Graeme Newman,*** *chief innovation officer, CFC Underwriting*

"Now companies have got the internet of things devices within their production facilities and rely on connected functionalities for critical operations," she said. "Additionally, we all used to have manual work-arounds for processes that were somewhat connected.

"But now we have all dismantled those work-arounds in favor of 'smart' processes. That means that if something 'smart' breaks, there's no other way to complete the task, so the BI loss gets worse."

The problem has been exacerbated because companies rely so heavily on these interconnected systems to run their day-to-day business, leaving them susceptible to malware and ransomware attacks, said Graeme Newman, chief innovation officer, CFC Underwriting. But this has at least caused risk managers and companies to sit up and take notice of the problem.

"Following the surge in ransomware and destructive malware that we witnessed in 2017, the awareness of cyber risk among more traditional industries has risen," he said.

"For them, the exposure is more akin to the risks covered under their property policies, hence why they have turned to these to look for cover."

SUMMARY

- ***Using the same*** underwriter for property and cyber is advisable.
- ***The IOT is*** increasing cyber risk for factories.
- ***Property is an*** admitted risk; cyber an unadmitted risk.


We believe every customer deserves person-to-person support.
That's why, when you call PHLY, you'll speak with a real person. A professional with answers to your questions about coverage, paying a bill, making a claim, binding a proposal, even how to use the chat feature on our website. Along with quality coverage and claims service, how we interact with you is one of the many things that set us apart.
Now, real quick, let's get you the answers you need.
Call 855.411.0797 or visit ThinkPHLY.com
A.M.Best A++ Rating
Ward's Top 50 2001-2017
94.5% Claims Satisfaction
100+ Niche Industries
REAL PEOPLE.
REAL ANSWERS.
REAL QUICK.
PHILADELPHIA
INSURANCE COMPANIES
A Member of the Tokio Marine Group
Philadelphia Insurance Companies is the marketing name for the property and casualty insurance operations of Philadelphia Consolidated Holding Corp., a member of Tokio Marine Group.
All admitted coverages are written by Philadelphia Indemnity Insurance Company. Coverages are subject to actual policy language.

COVERAGE HEADACHE

Many companies have a standard property program and are only now waking up to the cyber threat following recent attacks. As a result, Marcin Weryk, underwriting manager, cyber and technology, XL Catlin, said there has been an increase in clients looking for more inclusive property policies with cyber bolted on.

But because of the mismatch between property being an admitted risk and cyber being non-admitted, it's often tricky to add on cyber, he said. Companies are seeking guidance on whether their property program will cover them for a cyber event, he added.

To overcome the problem, Stephanie Snyder, national cyber sales leader, Aon Risk Solutions, said that companies need to use the same underwriter to provide their property and cyber coverage to ensure the two are streamlined. The need to work with specialist property and cyber brokers and carriers is also paramount.

"Many carriers are now making sure that any type of cyber risk that's bolted on to their property policy is written by the same underwriter," she said.

"It helps to give them a better aggregation of risk and eliminate any gray areas or overlaps in coverage."

A greater problem, said Newman, is carriers' understanding and appetite to insure these risks. Given the limited knowledge of cyber risk and a fear of aggregation, he said, often the only alternative has been for companies to turn to the excess and surplus market.

"The very real fear that one piece of malware could result in simultaneous limit losses across a huge property portfolio is what is preventing more insurers from entering this market," he said.

"Had NotPetya been targeted at the U.S. rather than Ukraine, then we could have witnessed an economic impact well in excess of $50 billion, much of which would have fallen on the property market had they provided affirmative cover for cyber risk."

STREAMLINED SOLUTIONS

Despite this, great strides have been made in aligning property and cyber coverage, said Tom Reagan, managing director and cyber practice leader, Marsh. But there's still a long way to go.

"Brokers and carriers have done a great deal of work over the last few years to try to align the two coverages. In general, the property market has continued to be responsive to physical events arising from cyber attacks, but on the other hand, the property market has been moving towards excluding non-physical cyber events," he said.

Companies also need to work with their brokers and carriers to identify any gaps in their programs, said Weryk. At the end of day, he said, risk managers must decide between an overarching policy covering all cyber and property risks or having separate ones.

"They have to make a clear decision as to whether they go for numerous separate policies or explicit coverage using one program," he said. "Both have merits and drawbacks, but it's up to them what suits their business."

Education is another key area to help companies, said Grace Reis, VP, cyber risk insurance products, FM Global. She said clients and brokers need to understand how their policy will respond to an event.

"You need to put in the groundwork before an event happens," she said. "The last thing you want is to get a nasty shock at 2 a.m. Companies need to treat cyber as an enterprise risk that affects all operations rather than just an IT issue. In a business sense, cyber and property may live in two different segmentations, but companies need to ensure they are plugging that gap." &

ALEX WRIGHT is a freelance editor and writer based in the UK. He can be reached at riskletters@lrp.com.