SILENT CYBER: AN ISSUE MAKING NOISE ACROSS INDUSTRIES AND COVERAGE LINES

CONTACT

To learn more about how AmWINS can help you place coverage for your clients, reach out to your local AmWINS broker.

LEGAL DISCLAIMER

ABOUT THE AUTHORS

This article was written by Kasey Armstrong and Megan North, professional lines brokers with AmWINS Brokerage in Seattle Washington and the creators of CyberUP.

As cyber events evolve in sophistication, scale and frequency, property and casualty line carriers are growing concerned about the potential for unintended claims. These cyber risks, which property and casualty carriers have neither underwritten nor charged for, can substantially increase their portfolio exposure. In response, many insurers have adopted various exclusions, sub-limits and changes to non-cyber insurance policies. This issue of non-affirmative coverage for cyber events is known as silent cyber.

Silent cyber incidents occur when coverage for a cyber-related loss is either inadvertently provided by insurance policies not specifically designed to cover cyber risk or the exposure is specifically excluded by the primary cyber policy or other policies, leaving coverage gaps.

Before chalking silent cyber up as something that won't impact your clients or may only be important for retailers that place professional lines accounts, take a look at a few coverage line and industry-specific examples.

WHEN CYBER EVENTS CROSS INTO PROPERTY AND CASUALTY

While you may primarily associate cyber-attacks with financial losses, today's cyber events can also result in first or third-party physical damage or bodily injury. For example:

- **Property:** Network interruption caused by a ransomware attack takes a critical HVAC system offline at a fruit warehouse. This causes temperatures to peak beyond optimal thresholds, resulting in damage to the housed goods as well as the facility itself.
- **Casualty:** A manufacturer's industrial control system is hacked and manipulated remotely to speed up the belts. This results in an overload at workstations and injury to workers.

When situations like these happen, what policy covers the claim? This is the fundamental question behind silent cyber and why retailers placing property and casualty policies should be aware of the issue.

HOW SILENT CYBER CREEPS INTO VARIOUS INDUSTRIES

Healthcare

Düsseldorf University hospital fell victim to a ransomware attack that crippled their entire technology network.

With the hospital's systems offline, there was a major disruption to patient care, including rerouting ambulances to other nearby hospitals. As with most ambulatory rides, time is of the essence, and during the event, a patient in critical condition died while in transit.

(continued on next page)

(continued from previous page)

In this case, a cyber-attack led to a tragic fatality. When lawsuits are filed for events like this, where can the hospital look for insurance coverage?

- Most cyber policies available on the market today include exclusions (or sublimits at best) for bodily injury and property damage losses.
- A medical malpractice policy would likely not apply, because the event did not arise from an error in treatment or medical advice. It is also important to note that cyber exclusions are being added to E&O policies more frequently.
- A general liability policy may not respond because loss arising from cyber events are commonly excluded.

In summary, non-cyber lines generally exclude cyber as a trigger or peril; whereas, cyber policies oftentimes exclude bodily injury and property damage loss. When one excludes the loss and the other the peril, a silent cyber incident occurs.

Manufacturing

Mondelez International is a manufacturer of snack brands, including Cadbury, Oreo, Ritz, Triscuits, Toblerone and Tang. When NotPetya malware infected two of its servers, a significant portion of the company's global Windows-based applications were affected, as well as its sales, distribution and financial networks across the company. Mondelez experienced computer damages and supply and distribution disruptions totaling over $100 million in losses.

This cyber-attack led to significant business interruption as a result of first-party property damage to their equipment being "bricked." Where can manufacturers look for insurance coverage for events like this?

- Property policies often deal with "direct physical loss" and in this case the property was, in essence, unharmed. Further, in this example, the carrier disputed the claim due to a clause in the policy that excludes any "hostile or war like act" by any "government or sovereign power." NotPetya is widely viewed as having been a state-sponsored cyber-attack, with Russia the sovereign being put forward as potentially being behind the malware.
- Cyber policies are often focused on resulting financial loss. In this case, the bricked equipment resulted in a financial loss, but what about the actual bricked equipment that needs to be replaced? That equates to millions of dollars in equipment value that traditional cyber policies either exclude, or provide a minimal sub-limit, leaving the insured to shoulder the cost.

When you read the fine print, the property policy was the coverage that was not responding. A broadly written primary policy, or the inclusion of cyber umbrella policy, could have responded.

Marine/Transportation

A shipping industry leader, A.P. Moller-Maersk, reported a $300 million dollar loss due to a malware attack that affected three of their major businesses and crippled their logistics operations worldwide. The company not only lost revenue during the shutdown and subsequent slow period, they also had to invest in finding a way to continue business after their go-to systems were taken down by the attack as well as rebuilding their IT department.

This cyber-attack led to significant delays, lost business and reputational harm. Where can logistics and other transportation companies look for insurance coverage for events like this?

- Property insurance traditionally covers business interruption expenses, but only those arising from traditional property perils. Cyber exclusions are removing ambiguity regarding their intent of coverage.
- Bricked or disabled computer hardware likely had to be replaced, which is often excluded from property policies and small sublimits may exist on a cyber policy.

(continued on next page)

(continued from previous page)

Imagine if Maersk was unable to coordinate the movement of vessels which led to collisions or other damage. If the property, casualty and marine policies had cyber exclusions and the cyber policy has a property damage exclusion, there would be a silent cyber gap in coverage.

SUMMARY

Cyber events can happen to insureds of all sizes in all industries – just look at the recent SolarWinds hack and its far-reaching impact. These events don't always just result in financial loss but can also cause first or third-party bodily injury or physical damage. Therefore, silent cyber is not only an issue for retailers focused on placing professional lines policies, it's also imperative for property and casualty retailers looking to protect their clients.

AmWINS offers the only product on the market designed specifically to combat silent cyber incidents. CyberUP is a comprehensive cyber umbrella policy designed to fill policy gaps by dropping down, not overlapping, existing policies across multiple lines of coverage. CyberUP provides retailers and insureds peace of mind for whatever type of losses are triggered from a cyber event. Contact your AmWINS professional lines broker or visit amwins.com/cyberup to learn more.

Need help determining your insured's specific silent cyber exposure and whether they need CyberUP? We've developed a self-assessment tool to identify risk factors and deliver an easy-to-understand score that retailers can share with their insured.