COMMENTARY

MAY 2017

No More Tears: Insurance Coverage For The "WannaCry" Ransomware Attack

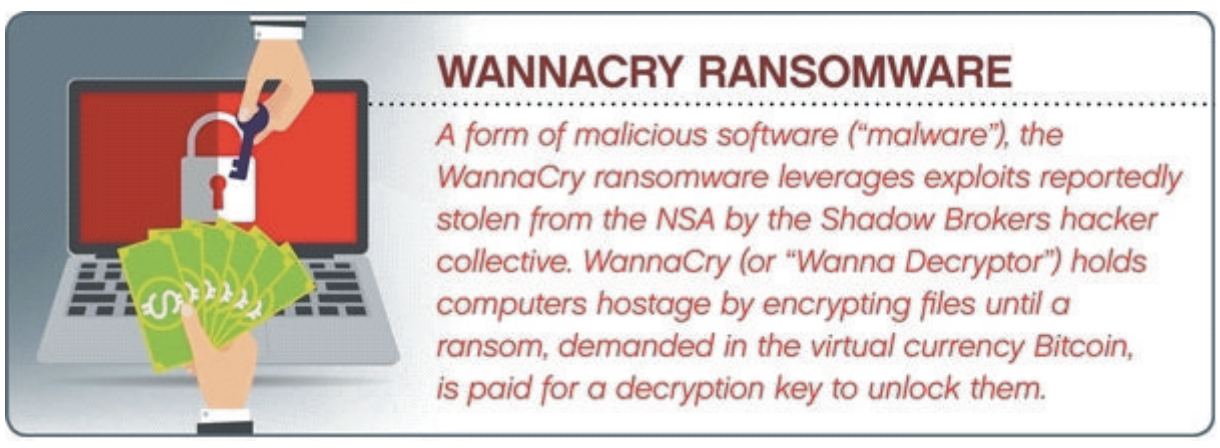
IN SHORT

The Situation: At least 300,000 computers in more than 150 countries were affected by the WannaCry "ransomware" attack.

The Result: Beyond the ransom demand, other expenses, inconveniences, and complications for victimized companies are likely.

Looking Ahead: Commercial policyholders should review their insurance coverage provisions before another ransomware attack occurs.

This month's WannaCry "ransomware" attack—the first truly global incident of its kind—is believed to have affected at least 300,000 computers in over 150 countries, claiming among its victims many large corporations and public entities. With business interruption losses estimated in the billions of dollars, the WannaCry attack has delivered a sobering reminder of the serious threat posed by cyber extortionists. The fact that such events are expected to continue with increasing frequency and sophistication only underscores the need for commercial policyholders to carefully review their insurance programs *before* the next ransomware event. Even companies with cyber insurance may encounter coverage challenges from their insurers with respect to ransomware attacks.



Review the Fine Print of Your Cyber Insurance Coverage Now

The potential losses caused by ransomware attacks can extend well-beyond the ransom itself to include forensic investigation and crisis management expenses, data repair and restoration costs, revenue loss due to the interruption of normal business activities, as well as third party liabilities. While other policies in your insurance program may respond with coverage for certain of these losses and should also be reviewed, particular attention should be paid to the scope of any cyber insurance coverage.

Cyber insurance policies typically contain insuring agreements addressing third-party liabilities (e.g., network security, privacy, and media liabilities) and incident response costs (e.g., forensic investigation, defense and crisis management costs, including customer notification and credit monitoring expenses). Some cyber coverages also provide insurance for first-party losses, including business interruption, the cost to restore lost or compromised data, as well as cyber extortion expenses.

Given that there are nearly 70 cyber insurers and no standard forms, policyholders should be aware that some cyber insurers may not include ransomware coverage in their basic form, but will include it upon request via endorsement. Therefore, it is important for risk managers to pay particular attention to the fine print of their company's cyber insurance coverage. As illustrated by the WannaCry attack, the billions of dollars in estimated business disruption losses dwarfed the approximately $300 per computer Bitcoin ransoms, the most significant economic losses to companies targeted by ransomware are often for related business disruption and forensic investigation costs. Risk managers should confirm that their company's cyber insurance policies adequately address these exposures.

> [P]olicyholders should be aware that some cyber insurers may not include ransomware coverage in their basic form, but will include it upon request via endorsement.

In addition, commercial policyholders will want to ensure that their cyber insurance policies are drafted broadly enough to capture both known and future forms of cyber extortion. For example, while cyber extortionists now commonly demand payment in the form of Bitcoin and other virtual currencies (or "crypto-currencies"), a number of cyber insurance policy forms have not been revised to specifically allow the payment of cyber extortion ransoms in such currencies. Where possible, policyholders should insist that their cyber insurance policies be drafted to expressly cover such modes of payment.

Policyholders should also review their cyber extortion coverage for any advance insurer consent provisions, which can apply not only to the payment of ransom demands, but also to forensic investigation and crisis management expenses necessary to investigate, evaluate, and address cyber extortion threats—thereby presenting an additional logistical hurdle for policyholders to face during such crises. While it is important for policyholders to be aware of such provisions, policyholders may be able to negotiate the deletion or modification of these and other provisions with their cyber insurers for no additional cost or only a modest increase in premium.

Policyholders should also be mindful of policy exclusions concerning their information technology operations. Some cyber insurance policies contain so-called "failure to patch" exclusions, which purport to exclude coverage for losses attributable to a failure to install or implement available software patches for known software vulnerabilities. Insurers may attempt to deny coverage for cyber-attacks where the policyholder used outdated software and did not implement security patches on a timely basis.

Cyber insurance policies also commonly exclude coverage for bodily injury—a consideration of particular importance to healthcare providers whose ability to deliver adequate patient care may be compromised during cyber extortion events. While the costs incurred by healthcare providers to investigate and end a ransomware attack may be covered, insurers may attempt to deny coverage for bodily injury allegedly resulting from the ransomware's impairment of healthcare providers' ability to provide medical services. In that event, affected healthcare providers may need to look to other policies within their insurance programs that insure bodily injury, such as professional and commercial general liability policies, which themselves may exclude coverage for cyber-related events. As this example illustrates, commercial policyholders will be well served to identify and address these potential coverage gaps in advance of the next cyber extortion incident.

FOUR KEY TAKEAWAYS

1. Cyber insurance policies vary significantly in scope.
2. The most significant losses to companies targeted by ransomware are often related to business disruptions and forensic investigation costs.
3. Ransomware attacks are often used to conceal broader hacking activities and theft of data.
4. In the event of a ransomware attack, policyholders should give notice of the event to their insurers under all potentially applicable policies as soon as possible.

WANT TO KNOW MORE
READ THE FULL VERSION.

CONTACTS


Tyrone R. Childress
Los Angeles


Richard DeNatale
San Francisco


Jason B. Lissy
New York

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**

"WannaCry": The Global Ransomware Attack

Time Is Money: A Remedy for Delay in Settlement of Commercial Insurance Claims in the UK?

The Road to Autonomous Vehicles: A Look at Insurance Implications

SUBSCRIBE SUBSCRIBE TO RSS