MARSH JLT SPECIALTY

INSIGHTS | **OCTOBER 2019**

Cyber Insurance is Supporting the Fight Against Ransomware

As the cyber insurance market continues to grow, it's only natural to discuss its place in the battle against cyber-attacks, including ransomware, which has been a prevalent topic in recent months.

Over the last several years, the cyber insurance market has rapidly expanded, and more companies now purchase cyber coverage than ever before. Close to 50% of respondents to Marsh and Microsoft's *2019 Global Cyber Risk Perception Survey* said they have cyber insurance, up from 34% in 2017. Amid that growth, most discussions of cyber insurance have highlighted its value as a risk mitigation tool and its ability to respond to fast-evolving cyber threats, including ransomware.

But in the media and elsewhere, some misinformation has emerged in regard to ransomware. One recent critique argues that cyber insurance has served as an incentive for cyber extortion attacks. In this line of thinking, the insurance industry is benefiting from the rash of ransomware attacks targeting companies around the world.

Under even modest scrutiny, this argument does not hold up. The truth is that ransomware attacks against businesses occur for one reason only: Criminals are succeeding.

That success stems from several factors. First, far too many organizations remain vulnerable due to gaps in technology or poor awareness of their risk. At the same time, ransomware attacks are cheap and easy to execute — and the criminals behind them usually operate in jurisdictions beyond the reach of law enforcement, where they are free to revise and repeat attacks as often as they wish.

Far from being part of the problem, cyber insurance can be a valuable tool in the fight against ransomware and other cyber threats. Fulfilling its traditional role, cyber insurance pools insureds that are similarly at risk and spreads their potential losses.

And those who have criticized it have gotten some important facts wrong:

- Ransomware victims are rarely "targeted." Why would they be? Targeting victims takes time, research, and money. A better strategy for attackers is to target a specific but widespread vulnerability that will quickly cause chaos and distribute links to ransomware to the maximum number of potential victims, and see who takes the bait. Each success is another quick smash and grab.

MARSH

- Insurance hardly creates an incentive for extortionists. As even critics concede, ransomware demands usually top out at five figures. For many businesses, that cost is a nuisance. And although no one wants to support cyber criminals, organizations are forced to weigh the option of paying ransoms against the risk of operational disruptions that could last weeks or months and cost far more. For example, after the City of Baltimore refused to pay a ransom demand of around $76,000, it incurred prolonged outages and racked up nearly $20 million in losses. Small and midsize businesses may not be able to absorb the same pain from a lengthy disruption. And if your company does not have cyber insurance to absorb those losses, you have even more incentive to pay.

- Insurers do not make decisions about whether to pay extortionists — the insurance buyer always makes the final call. The unfortunate truth is that — for many organizations — paying a ransom demand is the cheaper and more effective option. Even if cyber insurance absorbs the cost of a disruption, victims have many other considerations. How many initiatives will be sidelined as an organization flounders with its networks down? What happens to customers who depend on the services your company provides? What happens to your reputation? If an insured refuses to pay, its insurer supports the insured, paying network recovery costs and reimbursing it for income lost as a result of the attack.

Beyond its specific purpose in thwarting ransomware attacks, cyber insurance is valuable for other reasons. Before an attack occurs, the insurance underwriting process raises awareness of cyber threats, identifies how companies should be responding, and educates insureds. Cyber underwriters now demand much more information on how the companies they insure are combatting phishing attacks, which account for a large majority of cyber incidents.

After an attack, cyber insurance can also serve as a mechanism for convening the right team of experts, including legal counsel and computer forensic analysts, to assess the incident and recommend a response in a timely fashion.

So what do the critics get right? Just one important point: Cyber insurance pays claims. For more than a decade, cyber insurance policies have reliably paid claims for ransomware, network interruptions, data breaches, and related liability. Leading insurers handle thousands of claims a year, and US carriers paid cyber claims totaling an estimated $394 million in 2018.

Cyber insurance is, of course, not a complete solution. But it can be a valuable component in a larger risk management strategy that includes technology as well as training, education, and testing. To combat the scourge of ransomware, companies still need to teach employees how to recognize threats, patch regularly, limit user privileges, and establish sufficient cyber hygiene to avoid being an easy target.

Companies are fighting hackers on an unbalanced playing field, where defense is much harder than offense, and cyber insurance has proven to be a valuable partner in that fight. Given the stakes, companies should be eager to take all the help they can get.

This article first appeared on Brink News.

For further information on Marsh's cyber insurance solutions, visit marsh.com, send an email to cyber.risk@marsh.com, or contact your Marsh representative.

MATTHEW MCCABE
Senior Vice President and Assistant General Counsel for Cyber Policy
+1 212 345 9642
matthew.p.mccabe@marsh.com