Does It Ever Make Sense for Firms to Pay Ransomware Criminals?

By Chris Beck and Blake Fleisher

The global insurance company AXA announced in May it will stop writing cyber insurance coverage in France that reimburses customers for making payments to ransomware criminals. Cyber insurance policies have long covered these ransom costs, and it is widely anticipated that other insurance companies will follow suit.

While this news is important to companies as they value policies and understand their overall risks, it is also important news to the world of cyber bad actors. While the insurer's intent may be to reduce the incentives to conduct a ransomware attack by reducing the odds of the ransom being paid, the outcome likely will be more challenging.

When bad actors see that companies will not have the security of insurance coverage, they will likely make the economic determination of how much a firm would be willing to pay without the protection of insurance. Because this could lead to a reduction in the amount of the ransom, it follows that there would likely be an increase in the frequency of these types of attacks as the global network of savvy cyber criminals continue to evolve their tactics.

Ransomware hackers have often targeted large institutions such as hospital systems, government agencies and Fortune 500 companies, which are more likely to have the backstop of an insurance policy to cover the ransom demand.

Indeed, a representative from the ransomware gang REvil says insurance is "one of the tastiest morsels." In fact, REvil tries to "hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves," according to an article in The Record, a specialist cyber publication.

Ransomware has become one of the greatest operational threats to both the public and private sectors today. The Institute for Security and Technology Ransomware Task Force reports that firms are down an average of 21 days due to ransomware attacks, and it takes an average of 287 days for a business to fully recover from an attack. In 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware.

With AXA and potentially other insurance companies not renewing cyber insurance coverage when their customers pay ransoms, the strategic calculus for attackers and victims will change. When viewed from an economic perspective, firms need to make decisions based on the understanding that their data may not be restored and they may not cover their losses. Thus, if firms pay the ransom, they incur the hard cost of the payment itself with no assurance that their systems and data will be fully restored. Such an approach has the potential of mitigating any reputational damage.

Alternatively, if firms refuse to pay the ransom, they risk suffering loss of business, though this may be remedied by insurance. AXA's decision makes the calculation simpler for both the company and the bad actor: is the loss of business, even with insurance, more costly than the payment?

With insurance companies covering the costs of ransomware attacks, firms are incentivized to purchase this protection and, if hacked, pay the ransom. It has also been widely believed that ransomware attackers restore data when the ransom is paid because if they don't restore the data, firms would not pay them. However, this is not necessarily the case.

According to a recent survey by cyber security firm Sophos, "On average, orga-

nizations that paid the ransom got back just 65% of the encrypted files, leaving over one-third of their data inaccessible. 29% of respondents reported that 50% or less of their files were restored, and only 8% got all their data back."

With insurance companies not paying the ransom, companies will have some interesting decisions to make. First, should they make the payments at all? There is a high probability that they will receive more than half of their data back, but they also have to pay for it out of pocket because the insurer would no longer cover it.

Then there is the question of whether they would be made whole by their insurer. Would their insurance cover the costs of business disruption, recovery, and remediation? Would paying the ransom out of pocket trigger insurance companies not to make them whole? The answers to these questions will have a major impact on their decision making about whether to pay a ransom.

The attackers are also paying careful attention to these sorts of questions. With firms unable to afford large ransoms in the absence of an insurer providing the funds, it would be expected that bad actors will lower the amount of the ransom demand.

However, bad actors are going to want to make at least as much money as they have before, so they're likely to ramp up the number of attacks. This move would allow the bad actor to price the ransom at just below the total cost of the insurance policy. Furthermore, with insurance companies not providing coverage for the ransoms, the attacks would be expected to increase, and, needing more targets, ransomware gangs are likely to become more indiscriminate. Looking to see which companies have coverage would no longer be worth the effort. This has the potential to put smaller firms at more heightened risk than before.

With the proliferation of ransomware, which has been rampant for quite some time, and the inability to transfer the risk through insurance, companies are going to need to change the way they manage their cyber risk—particularly through how they use their controls.

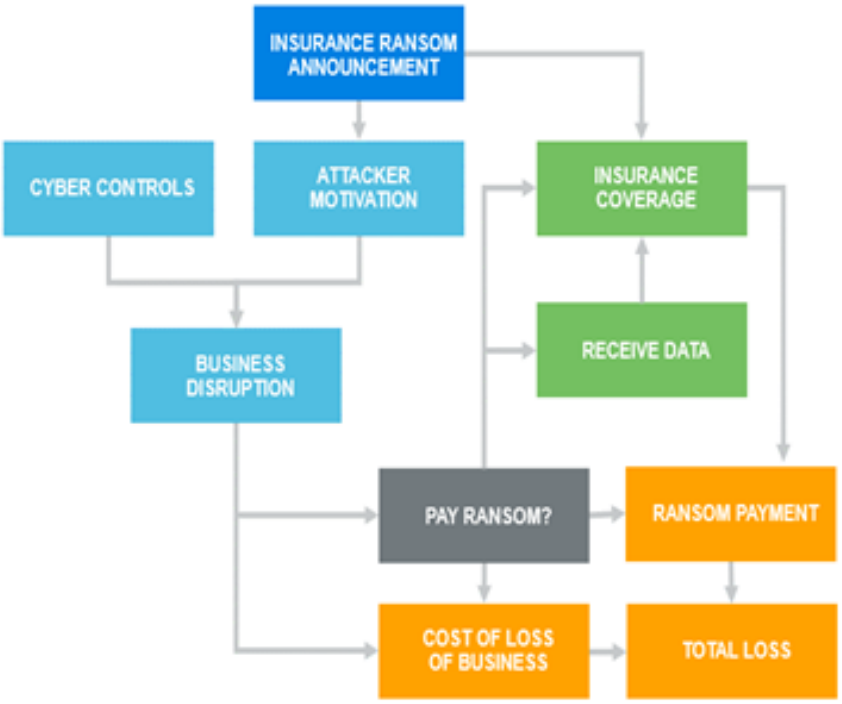

Figure 1: Ransomware Causal Model. Source: Milliman

Companies will likely turn to investing more in their cyber security controls. The challenge of mitigating the risk is not due to a lack of strategies, but rather to determining the appropriate amount of risk each company is willing to accept and which controls present the best business case to mitigate the risk.

To answer these questions accurately, the risk needs to be analyzed in a way that allows companies to examine the appropriate controls and mitigation techniques. Companies need to understand the business impact of their risk decisions to test and business case mitigation strategies to increase the probability of protecting a firm's assets.

The most effective way to quantify cyber risk and to understand the consequences of a risk mitigation or transfer strategy is to structure the analysis in a way that allows management to see consequences and trade-offs between the decisions. Causal-based models are a proven way to account for the decisions of both the company and the attacker, as well as detail the impact of their individual and, more importantly, their combined decisions.

In this simple ransomware example in Figure 1, the causal model can account for the various decisions made by the attacker, the insurer, and the target firm. Senior management can see how paying the ransom would impact the total cost of the breach, whether or not the firm receives its data back from the attacker, and making a claim under its cyber insurance policy.

With this type of modeling available, firms can make more informed risk decisions based on their cyber risk appetites, cyber security controls, and risk transfer options.

Chris Beck is the managing director of Milliman's Complex Risk Solutions practice. Beck has more than 16 years of risk experience in consulting and as a practitioner.

Blake Fleisher is senior cyber risk analyst at Milliman's Complex Risk Solutions practice. Blake is an Associate of (ISC)² and holds a master's degree in computer science from the University of Chicago.