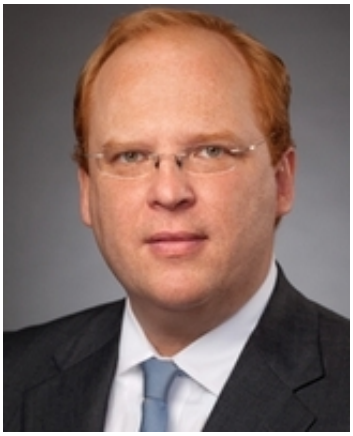
BETTER RISK MANAGEMENT RESULTS IN CHEAPER CYBER INSURANCE

December 7, 2014 - 6:00am



Christopher Brubaker

Applying a methodical approach to identifying cyber strengths and vulnerabilities at all levels of a company — from administrative to technical — will give a risk manager a strong hand when the time comes to purchase cyber insurance, an increasingly complex endeavor, says attorney Christopher Brubaker of Clark Hill P.L.C.

Now more than ever, risk management is a key component of any successful business. Diligence and attention to detail have always been key aspects of a successful risk management program. When it comes to cyber risk, these attributes have the potential to save you hundreds of millions of dollars.

Cyber risk is a complex and multifaceted threat that goes beyond compliance, which can be challenging enough in its own right. It encompasses a variety of internal and external threats that can be combined either by design or bad fortune. Organized gangs of cyber criminals are actively probing and attacking computer systems, exploiting any weakness they can find and constantly adapting to circumvent the latest technology. Your company may also be in the crosshairs of a foreign government and all of the resources a country can throw at defeating your cyber defenses.

Proactive risk management is the key to keeping these threats in check.

What is known to date about last year's Target Corp. breach illustrates the importance of risk management as it relates to cyber risk for policyholders and insurers alike.

Several months before the breach, Target installed a security system that provided a virtual environment for programs and processes to run before they were allowed on the main system. This provides the opportunity to identify and eliminate threats before they reach breach status.

The system reportedly did detect the malware that was used in the attack and issued warnings before data began leaving the system. However, the warnings were not acted on before the incident escalated and became a breach.

What is unclear at this time is exactly what the breakdown was with the risk management process that had been put in place. Target had clearly been proactive in trying to thwart the very risk that it fell victim to and yet still managed to succumb to this attack. Target's experience demonstrates both the benefits and limitations of risk management.

The Home Depot Inc. and Target data breaches also show the potential magnitude of losses related to a data breach. The types of loss are varied, numerous and can quickly escalate. There are a number of different figures being reported for the cost of the Target breach to date. Some reports put estimated losses at $148 million, with $38 million of that recoverable from insurance. Other reports put the total at $235 million, with $90 million paid by Target's cyber insurance. Reading these together suggests that Target has exhausted its cyber cover and been able to recoup some costs from other insurance, leaving it with a net loss of at least $110 million.

Home Depot's data breach (56 million payment cards) is significantly larger than Target's (40 million payment cards). Home Depot reportedly has $100 million in cyber coverage on top of a $7.5 million retention. If Home Depot's cost ratio is the same as in the Target breach, then Home Depot could be facing a net loss over $200 million.

Cyber insurance is here, and it is growing fast. A recent report estimated that $2 billion will be spent on premiums for cyber insurance in 2014, up 67% from 2013. Combine that with surveys indicating that only 26% of companies have cyber insurance, and those figures will only continue to rise. In many ways, this increase in demand is occurring at an opportune time with casualty and property policyholder surplus recently hitting all-time highs. However, risk management will be critical as this coverage continues to evolve — not only because of the lack of prolonged loss history and the potential magnitude of losses, but also because of the ever-changing nature of the risk.

With a large breach carrying costs that can easily exceed $200 million, how much cyber coverage is enough for your company, and will you be able to afford it? The amount of coverage needed will obviously vary greatly from company to company based on a number of factors. However, both the rate for the coverage and the limits available, whether for $20 million, $50 million or $200 million, will likely depend

primarily on risk management.

When it comes to underwriting for cyber insurance, risk management is the name of the game. Applications are in the nature of information technology risk management audits.

Illustrating this is the recent announcement of a new cyber insurance product in a partnership between Guy Carpenter & Co. L.L.C. and Ridge Insurance Services, led by Tom Ridge, former U.S. secretary of Homeland Security and governor of Pennsylvania. The product is aimed at small and medium businesses with limits up to $50 million and is being underwritten by a number of cyber-focused syndicates at Lloyd's of London. According to the Guy Carpenter news release, one of the key features is an initial on-site assessment of existing cyber security capabilities to be performed by Ridge Insurance Services. The assessment will include recommendations for improving security. How well those recommendations are followed will directly affect premiums.

Need more incentive to upgrade your cyber risk management? The results of a Ponemon Institute L.L.C. study show the average cost of a data breach at $201 per record. This cost can be reduced by $10 per record by having a chief information security officer and up to another $17 per record by having incident response plans in place prior to the breach, the study shows.

A final point to keep in mind is that cyber security protocols are essentially a risk management process. Most standards follow similar patterns. First, identify your cyber assets and their vulnerabilities. What data, systems and/or operations do you have that are part of your business process? How valuable or important are they to your business? What risks do these assets face?

Next, identify the processes, safeguards and controls that are in place or available. Remember to look at all methods: administrative, organizational, physical and technical. Subsequently, a cost-benefit analysis is in order to develop the plan that is right for you.

After implementing the plan, it is time to monitor, monitor, monitor. Stay vigilant, as threats will change, often quickly, over time. Respond to any and all anomalies that are detected. Remain flexible and always look for ways to improve.

Remember that the cyber-criminals are waiting for you to make a mistake.

Christopher Brubaker is an attorney with national law firm Clark Hill P.L.C. He has more than 15 years of experience in complex commercial and general litigation. He advises clients on insurance and reinsurance coverage, class action securities fraud, contract matters, business dissolution and insurance defense. He can be reached at cbrubaker@clarkhill.com and 215-640-8516.