PERSPECTIVES

CYBER RISK INSURANCE: WHY SIMPLY HAVING IT MAY NOT BE ENOUGH

BY **NANCY KELLY, COLIN N. HOLMES AND MATTHEW RICE**
> GOVERNO LAW FIRM LLC

As businesses grow and evolve in today's competitive landscape, many are finding that having a rational and comprehensive plan for responding to privacy crisis issues such as data breaches and cyber crime is of paramount importance. Cyber risk insurance coverage can play an integral part in how a company manages a data breach, however simply having coverage may not be sufficient to properly protect a business from all of the perils and costs associated with cybercrime. As the field of cyber risk insurance matures, policies are becoming more complicated, highly specific and customisable. It is critical that companies understand the intricacies of cyber risk insurance policies to ensure that they have the protection they actually need, and are not paying for unnecessary coverage.

Recently, several large companies such as Sony, Target and LivingSocial have been in the news for being the victims of data breaches in which personal information of their customers, employees or both has been stolen from their databases. Although these high profile cases consistently get more media coverage than smaller breaches, according to a recent study, the majority of worldwide data breaches actually occur at small companies ('2013 Data Breach Investigations Report', Verizon Risk Team) Increasingly, businesses of all sizes are realising the extent to which a data breach can harm their profitability, and many are taking steps to mitigate these risks by purchasing cyber risk insurance to supplement their existing CGL, E&O and general theft policies.

Traditionally, companies of all sizes purchase insurance policies to protect themselves from liability for errors, personal injuries, property damage and conventional crimes. Courts in the United States, however, have been split on whether these policies cover the costs and damages related to data breaches and cyber crime. Increasingly, businesses are discovering that traditional insurance policies are insufficient or completely inapplicable to the cyber risks that they are facing today, putting them in the precarious position of having to pay damages resulting from cybercrime directly out of their own pockets. Organisational costs for a single data breach average around $5.4m, or $188 per single record stolen, although this may vary by country and the type of damage resulting from stolen data ('2013 Cost of Data Breach Study: Global Analysis', Ponemon Institute). In order to protect companies from these increasingly expensive data breaches, more specialised cyber risk insurance coverage has emerged to fill the gaps in coverage of traditional insurance policies.

Cyber risk insurance is a relatively new product, and the scope of its coverage can vary from policy to policy. Additionally, since the market for cyber risk insurance is still developing, there is no industry-wide consensus on what these policies should cover. Various policies use different terms for the same products, and the absence of litigation in this area means that the legal system has not provided much guidance on the interpretation of cyber risk insurance policies. It is therefore the responsibility of individual companies to understand their existing protection, assess their risks and work with their insurance providers to tailor a policy for their specific business needs. By doing so, a company increases the likelihood that it has adequate coverage, and that it is not paying for unnecessary, insufficient or redundant policies.

> **"As the field of cyber risk insurance matures, policies are becoming more complicated, highly specific and customisable."**

In choosing a cyber risk insurance policy, several factors must be considered. Most importantly, companies must understand what types of damages a policy actually covers. Cyber risk insurance policies can cover an assortment of services, tools and remediation techniques relating to data breaches and cyber crime. Companies usually purchase

cyber risk insurance policies to protect themselves from losses suffered due to data breaches and the costs of managing the ensuing crisis. These costs can include hiring consultants to analyse the breach, notifying the potentially harmed parties in accordance to state and federal law, legal costs, ongoing monitoring of credit charges for affected parties, fines for being in breach of regulations, and rebuilding compromised security systems. Companies need to review their cyber risk policies carefully to ensure protection in each of these areas. Furthermore, while these may be the chief costs that companies associate with data breaches, they should consider other, more specific forms of cyber risk insurance that may be necessary to cover additional damages resulting from cyber crime.

As more companies store information online in 'the cloud', and engage third party vendors to manage such data, insurance issues arise when that data is lost or stolen. In response to these issues, some carriers have begun to offer cyber risk insurance products that can provide protection against cloud-based data breaches. Businesses should not rely on the cloud storage companies' insurance policies to cover all of the losses from a cloud data breach, as a company can incur costs associated with such a breach even when the data breach was the fault of the third party service provider. Costs can occur from the temporary inaccessibility of data, recovering stolen data, or transferring data to a new cloud storage system after a breach. By ensuring that overall network security and breaches of information stored by third parties in the cloud are covered in a cyber risk policy, companies can decrease the risk that a data breach, even in the hands of a third party, will come with unforeseen or unmanageable costs ('An Introduction to Cyber Liability Insurance Cover', ComputerWeekly.com, July 2013). Companies must also understand the intricacies of their cloud-based risk coverage, for some policies contain sub-limits that cap the amount of damages that will be reimbursed by the insurer. Knowing whether a policy has sub-limits for specific risks, such as cloud-based data breaches, is an integral part of obtaining adequate protection from cyber risk.

Insurance providers also offer cyber risk products that insure against the loss of revenue due to data breaches or cyber crimes. Known as digital business income coverage, this product protects against income that is lost or unrealised because of security breaches, website failures or cybercrimes that inhibit or prevent a company from doing business digitally or online. Most traditional business interruption policies only cover damages outlined in the general insurance policy, such as floods, fires or interruptions to the supply chain due to physical damage. Similarly, if a company's business insurance does not cover cyber crimes or data breaches, their business interruption insurance may not cover these losses ('Business Interruption Insurance: What it Will – and Won't – Cover', Entrepreneur, 16 November 2012).

Companies should consider whether digital business income coverage is a good fit for their business, as standard cyber risk policies may not include it. A company should not assume that lost revenue is included in a business interruption policy or even a basic cyber risk insurance policy. Discovering a lack of coverage in this area after a costly breach or cyber crime can be fatal to a company.

Another product available to companies purchasing cyber risk insurance is extortion liability coverage. Similar to traditional kidnap and ransom insurance used by companies with employees working in unsafe or politically unstable locations, extortion liability insurance protects businesses against the costs related to cybercriminals stealing confidential information and demanding payment for its return. While traditional policies usually only cover the kidnap and ransom of an actual employee or associate of the company, extortion liability coverage can be specifically tailored to cover ever-increasing cyber risks that arise when doing business online and in the cloud. Companies should evaluate whether obtaining extortion liability coverage is warranted for their business and know that basic cyber risk insurance coverage may not cover it.

Many factors go into choosing whether or not to purchase cyber risk liability insurance, including the risks of a particular business and the costs of such policies. However, the decision does not end with simply agreeing to purchase a policy. Due to the relatively new market for these products, the lack of uniformity between policies and the shortage of judicial decisions interpreting them, policies may not always cover what a company thinks they cover. Different terms are often used for the same insurance products, and assuming a product is covered by a certain policy can lead to disaster. Depending on their business model, companies need to consider tailoring a policy to include specific coverage for the direct cost of a data breach, costs relating to information managed or stored by a third party in the cloud, lost revenue and extortion. RC

Nancy Kelly
Partner
Governo Law Firm LLC
T: +1 (617) 532 9214
E: nkelly@governo.com

Colin N. Holmes
Associate
Governo Law Firm LLC
T: +1 (617) 737 9930
E: cholmes@governo.com

Matthew Rice
Law Clerk
Governo Law Firm LLC
T: +1 (617) 737 9215
E: mrice@governo.com