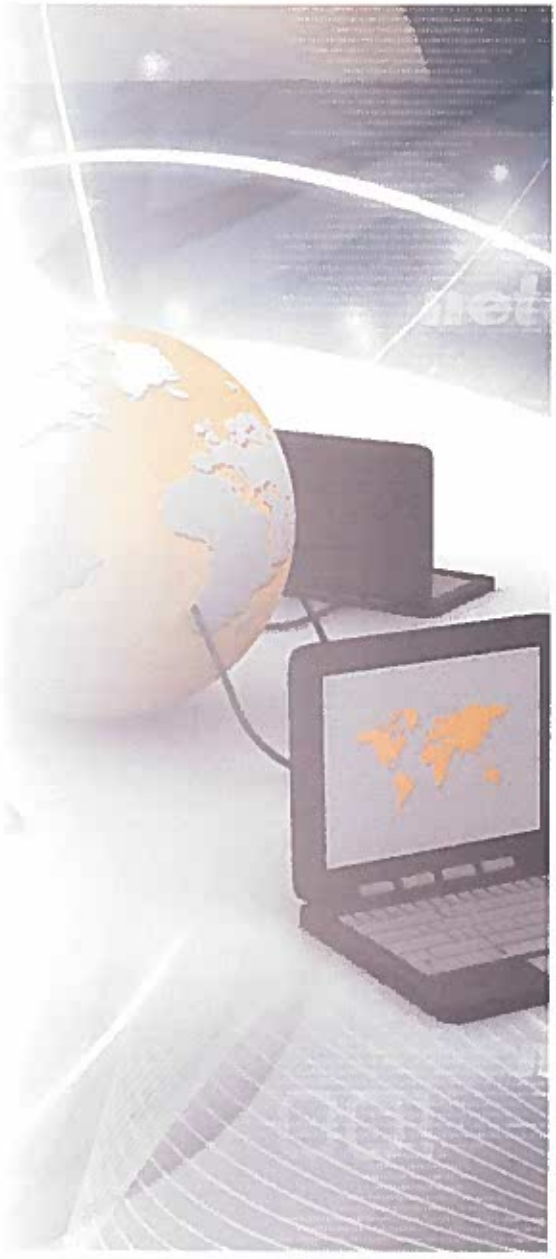
ONE-ON-ONE INTERVIEW

CYBER RISK INSURANCE COVERAGE



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

Nancy Kelly is a partner at Governo Law Firm, with a focus on complex litigation, coverage, and compliance matters, including data privacy and security. Prior to joining the firm, Ms Kelly served as legal counsel for a reinsurance services provider in London, where she specialised in coverage disputes, regulatory compliance and corporate transactions. She is a member of the International Association of Privacy Professionals (IAPP). Ms Kelly is admitted to practice in several US states, and is a qualified solicitor in England and Wales.

RC: To what extent are cyber risks and related liabilities increasing for companies and their D&Os? How vulnerable are companies to attacks such as data theft and hacking, data security breaches, computer network interruptions and privacy violations?

Kelly: Companies and D&Os face a significant risk of financial and reputational harm from data privacy breaches and cybercrime. A 2013 report by the Center for Strategic and International Studies estimated the annual cost of cybercrime to the US economy at $100bn. In 2013, the Ponemon Institute calculated that the average data breach in the US costs $5.4m. They also found that, for the first time, malicious and criminal attacks were the most frequent cause of data breaches in the US, at 41 percent, and the most costly, averaging a cost of $277 per stolen record. Employee negligence and system glitches persist as the remaining common sources of data loss. Such attacks and errors can result in significant financial penalties as a result of government investigations and enforcement actions, as well as private litigation and class actions. Perhaps even more dangerous for a company is the risk to its reputation after such a breach and the attendant media coverage. Companies need to consider and prepare for the growing likelihood of a cyber attack and data breach and take efforts to minimise their exposure and the resulting financial and reputational harm.

RC: Could you outline the principles of today's data privacy laws, and the demands they place on companies to implement security measures and follow notification requirements? How challenging is it for companies to maintain regulatory compliance?

Kelly: The regulation of data privacy is a complex web of state, federal, and international law, making compliance a complicated endeavour. There are several federal laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Gramm-Leach-Bliley Act (GLBA) that govern various aspects of data privacy. Generally, these regulations require an array of healthcare providers, businesses and financial institutions to establish safeguards for private information and create data privacy policies. They also empower agencies to enforce these rules. In addition to the federal framework, a majority of states have enacted data breach notification laws. Furthermore, a minority of states have created their own, sometimes stringent, data security regimes, requiring companies to implement specific data privacy protections. Several states have also adopted the Payment Card Industry Data Security Standard

(PCI-DSS), requiring merchants to protect credit card information. Companies doing business outside of the US must comply with international data privacy laws, notably the European Union Data Protection Directive, which governs data collection policies and requires particular privacy safeguards. In contrast to the US system, which is a series of intersecting industry and sector-specific laws, the European system focuses on the protection of an individual's privacy rights. Because these overlapping regulatory systems present myriad complicated issues, companies are well advised to retain outside counsel to ensure compliance and take efforts to minimise the risk of data breach and protect themselves from liability.

RC: For those companies that are yet to elevate cyber risk to a key area of focus, could you explain the kinds of reputational and financial damage that a breach can inflict?

Kelly: There are many types of reputational and financial damage a company will suffer in the event of a data breach. Direct financial damages can include network or website damage, data loss and business interruption. There may also be substantial financial costs involved in notifying consumers and responding to a breach. Government regulatory enforcement actions for noncompliance with data security laws and regulations, direct private litigation, and class actions can also take a massive financial toll. There have been several recent high profile data security class actions, including over 60 class actions against Sony, seeking damages of over $200m, a class action likely involving millions of individuals filed against comScore, and a suit against a New York hospital seeking $50m in punitive damages. Data breach suits are on the rise, with the class action bar devising and testing new theories of liability and damages as more cases are filed. Businesses face significant legal costs in defending such suits and the possibility of millions of dollars in damages. In addition to the direct financial costs of a breach, businesses can suffer great reputational harm, as breaches and lawsuits attract media attention and customers lose confidence in the company and seek goods and services elsewhere.

RC: What steps should companies take to establish appropriate processes and policies to manage cyber related risks?

Kelly: There are several steps companies can take to minimise the likelihood of data breach, limit potential liability and manage cyber risk. Companies should run regular attorney-directed risk assessments, in which existing data protection measures are evaluated against the legal and regulatory framework and problems identified before a data breach occurs. Businesses should also regularly update their policies and procedures

to determine the optimum way to protect private data, comply with relevant regulations and close any security gaps. These efforts should include instilling an understanding of data privacy issues in employees from the beginning and an ongoing effort to continue training employees to keep pace with changes in technology. Data is increasingly stored or accessed by new devices and on new platforms that can be vulnerable to breach, such as personal mobile devices and social media. Businesses should evaluate what private information they store and the potential risks of breach. While some companies will have greater risks than others, such as those involved in healthcare or retail, all companies have some risks. Another important step businesses can take is to establish policies to respond to data breaches when they occur, so they ensure compliance with notification requirements and quickly determine, and limit, the extent of the harm. Businesses can also create incident-response teams and have a plan in place to quickly respond to such breaches. Finally, organisations should consider the possibility of getting cyber liability insurance, which can mitigate some of the costs of data breaches should they occur.

RC: Insurance is a key part of managing cyber risk. What considerations should companies make when evaluating cyber coverage, including policy provisions and exclusions?

Kelly: Traditional insurance offers coverage for data breach and the loss of private information only under certain limited circumstances. Companies should examine their insurance coverage, including CGL, E&O, property and crime policies, and evaluate whether they provide coverage. There have only been a handful of cases interpreting these policies in the context of cybercrime and data loss, however, and it can therefore be difficult to anticipate whether traditional policies provide sufficient coverage. For many companies, cyber liability insurance may thus be the key to managing cyber risk. Such insurance is being offered by an increasing number of carriers and can apply to a variety of circumstances not included in traditional policies, including coverage for harm suffered by others due to the disclosure of

"Organisations should consider the possibility of getting cyber liability insurance, which can mitigate some of the costs of data breaches should they occur."

Nancy Kelly, Governo Law Firm LLC

confidential information, cyber extortion, regulatory compliance costs, data property costs of stolen or destroyed information, lost income due to cyber attack, and the costs of restoring lost data, notifying affected parties, pursuing a forensic investigation or defending against lawsuits.

RC: How would you describe pricing trends for cyber insurance? Are demand and competition dynamics leading to lower premiums?

Kelly: Over the past few years there has been a substantial increase in the number of businesses purchasing cyber insurance as the risks of cybercrime and data breach become more widely known and understood. Particularly there has been a spike in smaller companies purchasing such insurance. This rise in demand has resulted in a corresponding increase in providers and plans. Over 25 insurers now offer some type of cyber insurance, however the scope of coverage varies widely from insurer to insurer. Cyber insurance premiums appear to also vary significantly, with a recent report by Gartner, Inc. concluding that they can range from $10,000 to $35,000 for $1m in coverage. One reason for the difference in premiums is that carriers do not always have underwriters with experience regarding privacy losses and data breach and therefore insurers have difficulty pricing this insurance. Another reason is that because such insurance is a relatively new phenomenon, there have not been enough claims and payouts for underwriters to come to a consensus as to how this insurance should be priced. The price of such premiums will likely continue to evolve as more data breaches occur and claims are filed.

RC: What trends are you seeing in claims related disputes and litigation connected to cyber insurance policies? How are such disputes unfolding in this fairly nascent corner of the insurance market?

Kelly: There have only been a few cases interpreting if and when traditional insurance, such as CGL, E&O, property and crime policies, apply to incidents of cybercrime and data breach. Given the incipient nature of specifically-crafted cyber insurance policies designed to protect businesses in the event of data breaches, there have not been any reported claims-related coverage disputes on such policies or case law on these issues to date. It is certain that disputes on these policies will arise in the coming years, however at this point the law in this area remains undeveloped.

RC: What changes and developments do you expect to see in cyber insurance over the coming years?

Kelly: Cybercrime and data breaches show no sign of abating in the coming years, and with ever-evolving technologies and the prevalence of private information being stored by various businesses, there will likely be new challenges in protecting such information, new lawsuits related to such breaches, and new laws and regulations governing the protection of such information. An increase in the number of such incidents and the resulting publicity will likely result in a corresponding increase in the availability and variety of cyber insurance policies and a rise in the number of businesses purchasing such policies. As technology evolves, cyber insurance will need to evolve with it. For instance, already the shift by many businesses towards cloud computing has resulted in a debate among insurers as to whether cyber insurance covers a data breach of information stored in 'the cloud' by a third party. Some insurers are now offering specific cloud insurance, while others argue that it is covered by existing cyber insurance policies. Subrogation is also becoming an issue in cyber insurance, as insurers are increasingly evaluating suits against third parties, including cloud suppliers, contractors, and other service providers, that can be held liable for a data breach. Cyber insurance will no doubt continue to adapt and change to embrace these new challenges, and businesses must be vigilant in ensuring that their insurance policies cover potential liabilities and costs. RC