Message from the Chair

Dear Committee Members,

We have an action-packed program scheduled for the ABA Business Law Section Annual Meeting in Boston, September 8-10, 2016! I hope you will be able to join us at some or all of these events. The complete meeting program is available on the ABA website. Please check the schedule - it includes many CLE programs and complimentary networking opportunities.

The Director & Officer Liability Committee will have its regular meeting on Friday morning, September 9. The agenda will include updates on a number of ongoing projects, including reports on the potential impact on the advancement and indemnification rights of directors and officers under proposed amendments to the Model Corporations Act, current case law developments in director and officer liability, and director responsibility for Sustainability Financial Reporting.

Director & Officer Liability Committee Meeting
Friday, September 9, 2016
9:00 a.m.- 10:30 a.m.
Marriott Copley, Clarendon, Third Floor

Please use the following dial-in information if you cannot attend in person:

Toll-free dial-in number (U.S. and Canada):
(866) 646-6488
International dial-in number:
(707) 287-9583
Conference code:
1145265056

Directly following our Committee meeting from 10:30 a.m. to 12:30 p.m., we are co-sponsoring a CLE program with the Corporate Counsel Committee, entitled How to Maximize the Value and Reduce the Cost of Corporate Legal Services. The program will be held at the Marriott Copley, Grand Ballroom H1, Fourth Floor.

On Friday afternoon, September 9, we are also co-sponsoring a second CLE program with the Cyberspace Law Committee, entitled Director and Officer Liability and Cyber-Security: Questions Every Officer and Director Must Answer. The program runs from 2:30 4:30 p.m. in the Westin Copley, Courier, Seventh Floor.

And finally, be sure to attend the complimentary Section Welcome Reception on Friday evening, September 9, at 6 p.m. in the Westin Copley, America Ballroom North & Center, Fourth Floor. It is always a great event!

I look forward to seeing you in Boston,

Frances Floriano Goins
ULMER & BERNE LLP
Chair, Director and Officer Liability Committee
ABA Business Law Section
FLASH REPORT: Delaware Supreme Court Affirms Court of Chancery's Lack of Damages Award as an Exercise of Remedial Discretion in **OptimisCorp v. Waite**

By Brett M. Amron of Bast Amron LLP, Development Chair of the D&O Liability Committee

The Delaware Supreme Court recently issued its ruling in **OptimisCorp v. Waite**, C.A. No. 523, 2015 (Del. 2016). The opinion is noteworthy in that it provides practical insight for those who need to know the rights and obligations of directors who are appointed by written agreement as a condition of an investment in a company.

In **OptimisCorp**, the plaintiff corporation and its CEO, Alan Morelli, sought to recover $50 million in damages and other equitable relief. The plaintiffs alleged that the defendant directors had engaged in a conspiracy by intentionally failing to notify Mr. Morelli that an important amendment to the stockholders agreement, which would strip Mr. Morelli of his power to appoint a majority of the board, would be on the agenda at an upcoming special meeting of the board. When the meeting was held on October 20, 2012, the board voted in favor of the amendment, which ultimately resulted in Mr. Morelli's termination as CEO of the company.

Mr. Morelli subsequently filed a separate action pursuant to Section 225 of the Delaware General Corporation Law, which provides that upon application of any stockholder or director, or any officer whose title to office is contested, the Delaware Court of Chancery may hear and determine the validity of any election, appointment, removal or resignation of any director of any corporation and the right of any person to hold or continue to hold such office. The Court ruled expeditiously and sided with Mr. Morelli, invalidating his removal and the amendment to the stockholders agreement.

The Court of Chancery concluded that the plaintiffs were not entitled to any relief and dismissed all claims with prejudice. The Court of Chancery further ordered the parties to bear their own costs and declined to award damages to either side. The Court's decision was based on, among other things, its conclusion that the plaintiffs had engaged in misconduct that had threatened the integrity of the entire proceeding.

The Delaware Supreme Court affirmed the lower court's decision not to award damages. The Supreme Court, however, was explicit in stating that its affirmance was based on the fact that, because the amendment to the stockholders agreement was promptly invalidated as a result of Mr. Morelli's Section 225 action, the plaintiffs failed to show that they had suffered any additional non-speculative harm.
Despite the affirmance, the Supreme Court disavowed the Chancery Court's labelling of Mr. Morelli's claim as resting on a "super-director" theory, in which directors who have large stockholdings and the accompanying right to elect directors have "special rights" as super-directors. In the Supreme Court's view, such a tendentious description obscured the core issue, which was whether all directors are entitled to fair and non-misleading notice of the agenda for a special meeting. To that end, the Supreme Court stated: "Be it a director with a controlling interest or a director with only a handful of shares, we are uncomfortable embracing the idea that cliques of the board may confer and sandbag a fellow director." The Supreme Court went on to state, "it has long been the policy of our law to value the collaboration that comes when the entire board deliberates on corporate action and when all directors are fairly accorded material information."

FLASH REPORT: Advancements of Fees for Former Officers
By Brett M. Amron of Bast Amron LLP, Development Chair of the D&O Liability Committee

The following is a reposting of the Advancements of Fees for Former Officers written by Brett M. Amron, Development Chair of the D&O Liability Committee for the Business Law section of the ABA.

In Marino v. Patriot Rail Company LLC, C.A. No. 11605-VCL (Del. Ch. Feb. 29, 2016), the Delaware Court of Chancery confirmed that, under Section 145 of the Delaware General Corporation Law (the "DGCL"), the advancement and indemnification rights of officers and directors for actions taken while serving in that capacity: (i) continue after an officer or director leaves office; (ii) do not cover actions taken after an officer or director leaves office; and (iii) cannot be amended or eliminated retroactively unless the source of such rights explicitly provided otherwise at the time coverage was authorized or ratified. The opinion is also noteworthy for underscoring the importance of parties addressing how to deal with the issue of contingent liabilities—for example, pending litigation—in connection with the purchase of a company.

Patriot Rail involved an underlying suit between Patriot Rail Company, LLC (the "Company") and Sierra Railroad Company ("Sierra"), which ended in favor of Sierra. Sierra moved to amend its judgment to add Gary Marino, the former Chairman, President and CEO of the Company, as a judgment debtor. Marino sought advancement from the Company to cover the legal expenses he would incur to defend against Sierra's efforts to add him as an individual party and collect against him as a judgment debtor. When the Company denied his request, Marino commenced this action seeking advancements of attorneys' fees and expenses; the Company answered, and the parties cross-moved for summary judgment.

Article VIII of the Company's certificate of incorporation stated: "This Corporation shall indemnify and shall advance expenses on behalf of its officers and directors to the fullest extent permitted by law in existence either now or hereafter." The parties agreed that had Marino been sued by reason of his status as an officer while he was serving in that capacity, the Company would have been obligated to provide advancements. The issue, instead, was whether this language in the Company's charter continued to cover Marino for the same types of claims after he ceased serving as an officer.

Because the Company's charter contemplated advancement "to the fullest extent permitted by law," the answer turned on the language of Delaware's indemnification and advancement statute. 8 Del. C. § 145. After looking at the statutory history of Section 145 and case precedent, the Court held that Marino was entitled to the requested advancements for actions he had taken while serving in his capacity as an officer of the Company.

The Court paid particular attention to three subsections of Section 145: Section
145(e), which authorizes advancement; Section 145(j), which addresses the extent to which a covered person's indemnification and advancement rights for actions taken during the person's period of service continue after the person has ceased to serve; and Section 145(f), which limits a corporation's ability to cause a covered person's rights to terminate after the person has served in reliance upon them.

The Court explained that Section 145 authorizes a corporation to grant mandatory advancement rights to officers and directors that provide coverage conditioned solely on an undertaking (Section 145(e)). Such rights provide coverage for actions taken by individuals during their service, even after the individuals have ceased to serve, and continue to provide coverage unless the governing provision specifically states otherwise (Section 145(j)). Moreover, unless the governing provision provides otherwise, the granted rights cannot be altered or eliminated retroactively with respect to prior actions, after a director or officer has already exposed themselves to liability by acting on the corporation's behalf (Section 145(f)).

**Featured Articles**

**Cyber Security & Risk Management, Annual Review 2016**  
*Originally Published in Financier Worldwide, July 2016*  
*By Frances Floriano Goins of Ulmer Berne LLP, et al.*

The current cyber risk environment is a fast moving place. As companies develop new internal cyber policies and legislators introduce new guidance to help protect businesses and their customers, they are often just fighting to keep ahead of malicious actors.

Cyber risks continue to evolve; from ransomware to spear phishing, it is imperative that organisations keep themselves abreast of the latest developments in cyberspace and establish suitable defences. Cyber attacks are a major enterprise risk. Failing to protect data, intellectual property and customer information can be hugely detrimental for any business.

**Read more...**

**Target's Directors and Officers Dismissed from Data Breach Lawsuit**  
*By Frances Floriano Goins of Ulmer Berne LLP, Chair of the D&O Liability Committee, and Gregory P. Stein of Ulmer Berne LLP*

Target Corporation's (Target) directors and executive officers can breathe a sigh of relief after a Minnesota federal judge dismissed derivative claims brought against them by Target shareholders, stemming from a data breach in 2013 in which hackers stole credit card and other personal information of tens of millions of Target customers. Davis v. Steinhafel, No 14-cv-00203 (D. Minn.). This decision provides useful guidance for directors and officers on the issues a court may consider in determining whether to allow a derivative suit to proceed based on alleged violations of fiduciary duties in overseeing corporate cybersecurity.

**Read more...**
Financier Worldwide canvases the opinions of leading professionals around the world on the latest trends in cyber security & risk management.

Contents

**UNITED STATES**
Frances Floriano Goins
ULMER & BERNE LLP

**CANADA**
Vanessa Coiteux
STIKEMAN ELLIOTT LLP

**MEXICO**
Fernando Roman Sandoval
PWC

**UNITED KINGDOM**
Anita Bapat
HUNTON & WILLIAMS

**FRANCE**
Claire François
HUNTON & WILLIAMS

**SPAIN**
Carmen Segovia Blázquez
AON RISK SOLUTIONS

---
Contents

PORTUGAL ................................................................. 32
Leonor Chastre
CUATRECASAS, GONÇALVES PEREIRA, RL

BELGIUM ................................................................. 36
Wim Nauwelaerts
HUNTON & WILLIAMS

GERMANY ................................................................. 40
Dr Jochen Lehmann
GORG

AUSTRALIA ................................................................. 44
Emma Osgood
BERKSHIRE HATHAWAY SPECIALTY INSURANCE

SOUTH AFRICA ............................................................ 48
Jason Gottschalk
KPMG SERVICES (PTY) LTD
The current cyber risk environment is a fast moving place. As companies develop new internal cyber policies and legislators introduce new guidance to help protect businesses and their customers, they are often just fighting to keep ahead of malicious actors.

Cyber risks continue to evolve; from ransomware to spear phishing, it is imperative that organisations keep themselves abreast of the latest developments in cyberspace and establish suitable defences. Cyber attacks are a major enterprise risk. Failing to protect data, intellectual property and customer information can be hugely detrimental for any business.

In addition to their operational impact on an organisation, cyber attacks come with cost implications and can ultimately damage a company’s reputation in the eyes of customers and the wider world. The stigma arising from a data breach can be difficult to overcome.

Unsurprisingly, cyber security risk management is vaulting toward to the top of the corporate agenda. Though companies have been slow to awaken to the dangers, many are now taking their security responsibilities seriously and educating employees on risks and mitigation techniques. By establishing a culture of cyber security awareness, and training staff to identify security risks, companies can go a long way to protecting themselves and their data.

The emergence of cloud computing has had a significant impact on cyber security, and requires companies to develop a comprehensive risk management plan. The location in which companies store their data is critical in terms of relevant local legislation. Further, businesses must ensure that cloud providers are up to the task.

Cyber insurance, too, has a significant role to play in risk management. Businesses need to consider their options carefully and refrain from cost cutting when arranging cover; negotiating the right policy for their individual needs is key.
Q HOW WOULD YOU SUMMARISE TODAY’S CYBER-RISK ENVIRONMENT? WHAT NEW RISKS HAVE EMERGED IN THE PAST 12-18 MONTHS?

GOINS: Companies are becoming more secure, but no company is immune from breach. Cyber risk remains an enterprise risk because of the potential operational impact, cost and reputational harm a cyber attack can cause. In addition to continuing threats such as hacked systems, malware and phishing, increasing threats arise from ransomware and business email compromises. Ransomware is a malicious software that encrypts a victim’s data, making the data inaccessible and holding it for ransom until the victim pays a cash ‘ransom’ for a decryption key. It is profitable because the cost of losing or restoring the data is often higher than the ransom payment. Business email compromises, such as a criminal posing as an officer of a company – such as the CEO – and sending an email instructing a company employee – such as the CFO – to quickly wire funds to a specified bank account for a plausible business transaction, are another growing threat.

Q WHAT IMPACT HAS THE CLOUD HAD ON DATA SECURITY? WHAT SHOULD COMPANIES BE CONSIDERING WHEN TRANSFERRING DATA STORAGE TO THE CLOUD?

GOINS: Data security is no longer only about protecting corporate networks. Companies must protect their data anywhere it resides, no matter who controls it. The ubiquitous use of cloud services has substantially expanded the scope of security responsibilities, forcing companies to examine the security provided by each cloud service provider handling their data. If data will be less secure in the cloud, companies should carefully consider whether the use of the cloud service is appropriate. On the other hand, cloud providers may offer better security than an organisation is able to provide itself, particularly smaller organisations, so the use of a cloud service may actually improve data security. Regardless of the reputation of the cloud service provider, the terms of the service contract are critical. At a minimum, companies must thoughtfully review the terms of the cloud agreements and insist upon adequate protections in case of a security breach.
Q COULD YOU OUTLINE THE PRINCIPLES OF DATA PRIVACY LAWS IN THE US, 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?

GOINS: In the US, there is a patchwork of data privacy laws and compliance obligations that differ by industry. In addition, most of the 50 states have their own laws and regulations, mostly designed to protect consumer privacy and report breaches. Organisations such as financial institutions and healthcare providers operate under well-developed regulatory frameworks, and are generally further along in protecting information and coping with breaches. At the opposite end of the spectrum, manufacturing companies engaged mainly in business to business transactions and that are primarily subject to laws covering loss of employee personal data may fail to realise potential risks to their own commercial and business data. Companies doing business internationally may find themselves caught between responding to US regulators and observing stricter foreign privacy laws. The challenge to any US entity of identifying and complying with state, federal and foreign law applicable to its own situation is substantial.

Q WHAT STEPS SHOULD COMPANIES TAKE TO ESTABLISH APPROPRIATE PROCESSES AND POLICIES TO MANAGE CYBER RELATED RISKS? HOW IMPORTANT IS IT TO ADDRESS THE ORGANISATION’S RISK CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

GOINS: Cyber risk affects all aspects of the business, including significant financial, legal and operational issues. Its management cannot be left solely to IT. A multidisciplinary team can better address all relevant factors by analysing what data the entity holds, what data is critical to its business and possible ramifications of a breach. The entity’s risk culture, formed by appropriate board and employee training and cross-disciplinary communication, is critical. People remain the biggest threats to the maintenance of data privacy because employees are often able to bypass internal security controls. Although ‘top-down’ attention has been the mantra of late, recent studies suggest the training and example set by mid-level management may have a greater impact on employee activity. Thus, for any cyber security protocols to succeed there must be buy-in at all levels of the organisation and all employees must understand their duty to make responsible decisions and remain vigilant to evolving threats.
“Understanding cyber security issues is becoming essential to every board’s obligation in overseeing the company’s management and enterprise risk.”

GOINS: Insurance for cyber risk is still evolving from the older forms of technology errors and omissions and media liability coverage to privacy and network security coverage. About 50 insurers now offer some form of cyber insurance in the US, but it is important to review any policy carefully to assess actual coverage and exclusions. Coverage for a data breach in which customers’ personal information is stolen may also cover legal, public relations and loss of profits or other expense, but may not address the costs of regulatory investigations and fines, investigation and defence costs, settlements and judgments. Often, reputational harm, loss of future revenue and loss of the company's own intellectual property may not be covered. Many companies find that the process of going through an insurance assessment with a knowledgeable underwriter helps them to evaluate their current security protections, identify gaps and prioritise resources to improve security.

Q INSURANCE IS A KEY PART OF MANAGING CYBER RISK. HOW ARE INSURANCE PROVIDERS ADJUSTING OR ENHANCING THEIR INSURANCE SOLUTIONS TO MEET MARKET DEMANDS? WHAT TYPES OF POLICIES ARE AVAILABLE TO HELP MANAGE THE DOWNSIDE?

GOINS: Cyber liability insurance policies need to include protections tailored to the entity’s business. Before shopping for cyber liability insurance, a company must understand its business, how it stores and processes data, and the possible liabilities that can arise from a breach, including notification costs, litigation, regulatory fines and credit card fines. For example, if a company stores sensitive data with a cloud service provider, it becomes critical for that company to obtain cyber liability insurance that covers breaches affecting the parties that hold its data. Likewise, a company that processes credit cards must ensure that its cyber liability insurance covers potential claims from credit card companies relating to the breach. It is also critical for companies to carefully compare their needs to the actual policy under consideration. Some insurers or brokers advertise policies as providing ‘full cyber risk coverage’, while the actual policy may except costly potential liabilities, such as contractual obligations.

Q WHAT CONSIDERATIONS SHOULD COMPANIES MAKE WHEN EVALUATING CYBER INSURANCE COVERAGE, INCLUDING PRICING, POLICY PROVISIONS AND EXCLUSIONS?
GOINS: Cyber security is not a fad. Already a top-of-mind issue for directors, cyber security will become increasingly critical for the foreseeable future. All businesses are becoming more reliant on technology and will be collecting and storing more cyber data, while hackers become increasingly imaginative. Just as financial oversight has become an integral component of directors’ oversight responsibility and some boards have taken steps to include a financial expert among their number, understanding cyber security issues is becoming essential to every board’s obligation in overseeing the company’s management and enterprise risk. Boards are beginning to consider whether a cyber-expert director is also a necessary board component, or at least whether to assign a C-suite officer to oversee cyber security and report regularly to the board. Governmental actions like the US Cybersecurity National Action Plan and SEC guidance on disclosure of material cyber security risks and incidents will continue to push cyber security toward the top of board agendas.

Frances Floriano Goins co-chairs Ulmer & Berne’s data privacy & information security and financial services & securities litigation practice groups. Her practice includes counselling businesses on data privacy, cyber security, and corporate governance issues and resolving complex business disputes for public and private companies. She also defends clients in securities and financial regulatory proceedings, and has conducted numerous internal investigations. Ms Goins was tapped by the US Department of Homeland Security to address cyber security in the C-suite and boardroom in its C-Cubed webinar series. She is ranked in numerous peer-reviewed publications, and chairs the ABA Director & Officer Liability Committee.
**COITEUX:** I would say that in the past 18 months, we have witnessed a number of important developments. These include a jump in extortion-driven attacks where hackers use sensible information to blackmail organisations, new risks emerging from poorly planned or executed cloud service integrations or the use of non-secured cloud based solutions, an increase in risks posed by third-party suppliers and contractors having access to a company’s infrastructure, the proliferation of new and mass repackaging of ransomware, and security incidents related to enterprise connected personal and mobile devices (BYOD).

---

**COITEUX:** The cloud computing landscape has grown intensively in the last few years because of its relatively low cost and its functional and economic advantages over traditional storage methods. However, one thing to remember is that a company outsourcing data storage to a cloud service provider does not outsource its privacy obligations under Canadian privacy laws. As such, one primary concern is to ensure that the information sent to the service provider is protected. What are the safeguards used by the service provider to protect the data? What monitoring does the company do to make sure those safeguards are being implemented and followed? There are a few ways to reduce a company’s risk profile when using the cloud. Companies should be selective in the type of data transferred to the cloud. They should ask questions about the jurisdiction in which data is being stored and the legal and regulatory privacy requirements governing this jurisdiction. They should ensure that sufficient safeguards are implemented by the cloud provider, such as through contractual representations and covenants and rights of audit and access, as the case may be. Finally, they should include a clear allocation of responsibility and liability among the service provider and the client in the contractual documentation to avoid any gap or disconnect.
Q COULD YOU OUTLINE THE PRINCIPLES OF DATA PRIVACY LAWS IN CANADA, 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?

COITEUX: In Canada, the collection, use and disclosure of personal information in the private sector is either governed by federal, provincial or sectorial legislation, depending on many factors. All privacy laws, whether federal and/or provincial, require companies to implement sufficient security safeguards designed to adequately protect personal information. That said, most data privacy laws in Canada only establish general guiding principles to be followed by Canadian organisations. Currently, Alberta is the only Canadian province imposing a notification obligation in case of breach. However, the new Digital Privacy Act (DPA), once the regulation implementing its application is adopted, probably in Autumn 2017, companies that are subject to federal law will be required to, among other things, notify the Privacy Commissioner of Canada and affected individuals of any breach of their security safeguards involving personal information, if such a breach meets certain thresholds. They will also need to establish and maintain a record of every breach of their security safeguards involving personal information. While some companies were already notifying affected individuals on a voluntary basis, companies governed by the DPA will now be forced to do so. These new breach notification provisions will definitely result in new costs, risks and challenges for Canadian companies, including an increased pressure for transparency.

Q WHAT STEPS SHOULD COMPANIES TAKE TO ESTABLISH APPROPRIATE PROCESSES AND POLICIES TO MANAGE CYBER RELATED RISKS? HOW IMPORTANT IS IT TO ADDRESS THE ORGANISATION’S RISK

COITEUX: It is extremely important for a company to have a carefully crafted cyber security plan, including both a data security policy and an incident response plan. The data security policy should focus on three aspects. First, governance – ensuring that senior management and board members are accountable and allocate responsibility and resources. Second, industry standards – ensuring that the infrastructure is up to date with current security standards. Third, and, most importantly, corporate culture – raising level of awareness among the employees. Most security professionals would agree that many companies’ weakest link is, more often than not, their people. As
"Board members now realise that they have to take active steps if they want to fulfil their fiduciary duties."

CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

such, organisations must train their employees so they can understand the importance of cyber risk management, identify potential sources of cyber security breaches and know how to react when one happens.

Q INSURANCE IS A KEY PART OF MANAGING CYBER RISK. HOW ARE INSURANCE PROVIDERS ADJUSTING OR ENHANCING THEIR INSURANCE SOLUTIONS TO MEET MARKET DEMANDS? WHAT TYPES OF POLICIES ARE AVAILABLE TO HELP MANAGE THE DOWNSIDE?

COITEUX: Market demands are ever changing since new risks emerge every day and insurance companies build corresponding policies designed to address such risks. If everyone agrees that the average cost of a cyber breach increases year after year, it is still a challenge for insurance providers to adequately quantify the damages and related costs associated with a cyber attack and, incidentally, accurately assess their risk. Given the lack of historical data, especially in Canada, it is difficult to put a monetary value on cyber risk. Another challenge for insurance providers is the dynamic nature of cyber risks, which forces them to adapt their insurance offering to ensure coverage is always up-to-date. While it is true that cyber liability insurance is modular, the basic offering generally includes two components: first-party coverage for the companies’ own losses and third-party coverage for an insured’s third-party losses. Other cyber insurance features, such as business continuity coverage, may be added to cover specific business risks and needs. As a result, a cyber liability insurance product is not a one-size-fits-all product that suits every company’s needs, but rather is tailored to each company.

Q WHAT CONSIDERATIONS SHOULD COMPANIES MAKE WHEN EVALUATING CYBER INSURANCE COVERAGE, INCLUDING PRICING, POLICY PROVISIONS AND EXCLUSIONS?

COITEUX: It is no secret that, when evaluating any insurance product, a company has to look at inclusions and exclusions carefully. Since cyber crime is a risk that is so different to what insurers typically cover, traditional provisions of general liability insurance policies will sometimes burden the insured with unexpected exclusions. For example, is cyber crime considered terrorism? What if it is state sponsored? Other considerations that are specific to cyber risks also need to be taken into account. For example, would a company be insured against the damages resulting from malware installed on the company’s systems before the insurance was taken but which resulted in a cyber attack after the company was insured? Is the policy retroactive? Furthermore, as cyber insurance is quite complex, with tens of different risks...
coverages offered to companies, coverage needs to be assessed on a case-by-case basis based on every company's infrastructure, appetite for risk and risk profile.

**Coiteux:** Based on experience, in most organisations, boards only have one technology related discussion per year, or even less. However, we believe this is set to change, since we have recently noticed a rise in cyber security related questions asked by board members. The increase in the number of cyber attacks year after year, and the fact that technology and types of attacks evolve so quickly calls for more regular discussions on this topic. Board members now realise that they have to take active steps if they want to fulfil their fiduciary duties. In the current business landscape, breaches are inevitable but boards can mitigate risk and damage by staying informed and ensuring that, in the event of a breach, their companies are as prepared as possible to respond.

**Vanessa Coiteux**
Partner
Stikeman Elliott
+1 (514) 397 3681
vcoiteux@stikeman.com

Vanessa Coiteux is a partner in the Montréal office of Stikeman Elliott LLP. Her legal practice focuses on securities, public and private mergers and acquisitions and corporate financing. She specialises in cyber security and advises public and private companies on legal, ethical and governance issues. Ms Coiteux advises clients on a wide range of privacy, data security and information management matters, including information security breach responses, compliance and disclosure, and provides opinions on best cyber security business practices. She holds a LL.B. & B.C.L. from McGill University.
Q HOW WOULD YOU SUMMARISE TODAY’S CYBERRISK ENVIRONMENT? WHAT NEW RISKS HAVE EMERGED IN THE PAST 12-18 MONTHS?

ROMAN: Cyber risks in Mexico have definitely increased over the past two years. Today, there is a global trend of ‘targeted attacks’ with a clear economic interest – and Mexico has been no exception. This has forced organisations to make investments to face these new risks. The cyber risk environment is diverse, and certain industries are more vulnerable than others. However, in the last 18 months we have seen DDoS, DDoS extortion, ransomware, fraud, phishing and malware, among others. Currently, companies still see cyber security as an IT problem instead of a business problem. Organisations must adopt an approach that includes cyber issues in their enterprise risk management.

Q WHAT IMPACT HAS THE CLOUD HAD ON DATA SECURITY? WHAT SHOULD COMPANIES BE CONSIDERING WHEN TRANSFERRING DATA STORAGE TO THE CLOUD?

ROMAN: Using cloud computing services has had an impact on data leakage. When using these kinds of services, companies should first analyse the risks they are facing. Many companies feel that when they transfer information to the cloud, the service provider becomes responsible for the information, and they forget that they continue to be the information owner and responsible for its protection. With this kind of service, we have noticed that there are a lot of contractual gaps, as well as no clear definition or limitation of security measures that each party is responsible for. When transferring the information to the cloud, several risks have to be considered, and different controls included, such as securing transferring protocols, encryption and most importantly, taking into account other regulatory requirements when using the service.
Q) Could you outline the principles of data privacy laws in Mexico, 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?

ROMAN: In Mexico, we have the Federal Data Privacy Law, which focuses on getting data owner consent and ensuring that information is used for a legitimate purpose. Also, there are several laws that companies have to comply with in order to protect information, but from a security point of view. The Mexican Privacy Authority is releasing recommendations to companies as to the administrative, technical and physical security measures to implement, as well as the methodologies to follow to ensure data privacy according to several international standards. By law, companies are obliged to establish administrative, technical and physical security measures to protect personal information. In the Data Privacy Law, companies have to notify data owners if there is a vulnerability; however, how they must do this is not well defined and there is a lack of strong regulatory requirements to establish and define this type of notification. For some sectors, companies are obliged to report security incidents to their sector regulator, but from a security point of view. Currently, if companies have personal data vulnerability, these issues are notified to the authority or data owner. The Mexican authority is looking at this and is taking measures to sanction companies. Currently, data leakage is one of the issues with the highest sanctions rates in Mexico.

Q) What steps should companies take to establish appropriate processes and policies to manage cyber related risks? How important is it to address the

ROMAN: The first step is to create awareness among executive board members as to the importance and impact of the risks. The objective is to integrate these risks into their enterprise risk management. This should be followed by the adoption of best practices or worldwide approaches for information security risk management, for example, ISO 27001 or NIST, among others. With the sponsorship of the executive board members, it will be easier to create a strong security culture and to assign relevant roles and responsibilities. Companies have to take into consideration
ORGANISATION’S RISK CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

the current regulations by country or industry which they must follow to comply and ensure their information is well handled, and with an acceptable level of risk. In Mexico, there is a gap in security culture and awareness and it is important to address and change the mindset: to see information security as a business matter and not as a technology matter. Each employee must understand their role and responsibilities in case of any threat, and to ensure information security.

Q INSURANCE IS A KEY PART OF MANAGING CYBER RISK. HOW ARE INSURANCE PROVIDERS ADJUSTING OR ENHANCING THEIR INSURANCE SOLUTIONS TO MEET MARKET DEMANDS? WHAT TYPES OF POLICIES ARE AVAILABLE TO HELP MANAGE THE DOWNSIDE?

ROMAN: As with other types of risk, this treatment decision must consider the results from the risk assessment process, including the losses or impact the business could be subjected to and the probability of identified scenarios arising given vulnerabilities and threats. Although this is a policy that companies should acquire, it is, however, not very common in Mexico.

Q WHAT CONSIDERATIONS SHOULD COMPANIES MAKE WHEN EVALUATING CYBER INSURANCE COVERAGE, INCLUDING PRICING, POLICY PROVISIONS AND EXCLUSIONS?

ROMAN: Insurance companies in Mexico are starting to develop these kinds of products. We have to consider that much depends on the current regulations in each country with regard to privacy, the current economic environment and the evolution of cyber crime. The law in Mexico does not request these types of products. However, we are seeing an increase in cyber security threats, so the market is changing and starting to demand such products, although they are uncommon in Mexico. The type of policies now being offered in regard to the type of coverage depends on each client’s needs.
"Each employee must understand their role and responsibilities in case of any threat, and to ensure information security."

**Q GOING FORWARD, MAJOR CYBER THREATS ARE ONLY LIKELY TO INCREASE. DO YOU BELIEVE CYBER RISK MANAGEMENT WILL CONTINUE TO CLIMB THE BOARDROOM AGENDA?**

**ROMAN:** Cyber threats will definitely continue to grow and evolve. Mexico has become one of the key countries in which to invest, and this is one of the drivers on which attackers are starting to focus. As long as the economy grows and companies acquire more and new technologies, they will continue to face heightened cyber risks. So, seeing information security and cyber security as a business matter, and including it in the risk management process, will become one of the main issues on the executive agenda.

---

**Fernando Roman Sandoval**

Cyber Security and Data Privacy Partner
PwC Mexico
+52 55 526 5898
fernando.roman@mx.pwc.com

Fernando Roman Sandoval is an Information Security and Technology Partner in PwC Mexico within the IT Risk Assurance area. During the last 10 years, he has developed PwC Mexico’s Information security and technology services portfolio, through which he has provided support to clients concerning the strengthening of their risk management and compliance with different regulations which they are subject to. Mr Roman has participated in and managed numerous projects in different industry sectors including financial, public and consumer, among others. Mr Roman is the coordinator responsible for the IT Risk Assurance Innovation Group for PwC Mexico.
BAPAT: Cyber risk has proliferated in the last few years, with cyber crime growing not only in volume but in sophistication. As well as the more traditional actions, such as theft deployed by internal rogue actors, we are seeing a broad range of techniques being deployed by cyber criminals including phishing, denial of service attacks, malware, ransomware and persistent threats. Companies need to be aware of the heightened cyber risk and spectrum of threats that may be launched against them – often multiple attacks simultaneously – and implement appropriate internet and network security to ensure as high a standard of security as possible as well as robust internal policies and procedures to manage such risk.

BAPAT: The introduction of the cloud has raised specific data security and privacy issues which companies need to work through carefully before taking up cloud services. The location of the data is a key issue and, in many cases, the cloud provider will be established in a country outside the EU. In such instances, as the data will be transferred outside the EU, companies will need to implement an appropriate data transfer mechanism to permit such a transfer and ensure the appropriate security measures are imposed on service providers contractually. The use of subprocessors must also be dealt with and companies should ensure that any security obligations and data transfer restrictions that are imposed on cloud providers are imposed on any subprocessors too. Finally, as with the engagement of any service provider, companies should ensure they have audit rights, although with cloud providers this can be challenging due to the shared infrastructure and the confidentiality issues that arise. In any case, companies should ensure they have some form of audit rights.
Q COULD YOU OUTLINE THE PRINCIPLES OF DATA PRIVACY LAWS IN THE UK, 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?

BAPAT: The UK Data Protection Act 1998 places a requirement on companies to put in place appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss of, destruction of, or damage to, personal data. There are no specific measures that are prescribed but the level of security must be commensurate to the nature of the data and the potential risk of harm to the individual if the data was compromised. While there is no mandatory obligation to notify the UK Information Commissioner’s Office (ICO) of cyber breaches, the ICO recommends notification where a serious breach has occurred. This is not defined but guidance issued by the ICO states that the potential detriment to affected individuals, the sensitivity and the volume of the data compromised should be taken into account. An organisation suffering a cyber incident would need to think carefully about whether to notify the ICO.

Q WHAT STEPS SHOULD COMPANIES TAKE TO ESTABLISH APPROPRIATE PROCESSES AND POLICIES TO MANAGE CYBER RELATED RISKS? HOW IMPORTANT IS IT TO ADDRESS THE ORGANISATION’S RISK CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

BAPAT: In order to deal with an incident appropriately, companies should ensure they have in place an incident response plan which outlines all the key steps and considerations involved in the management and containment of a cyber incident. It would also be advisable to set up a dedicated incident response team with the relevant expertise to assist in such an event. This may comprise internal departments as well as external parties, such as forensic investigators to investigate the cause of the incident or lawyers who are able to advise on any obligations to notify customers or regulators. Companies may find it useful to simulate cyber incidents to test the effectiveness of their incident response plans and hone them accordingly. Separate from this, an organisation should be able to identify and categorise its data assets in order to establish which data pose the greatest risk. This will enable a company
“Companies will have to implement a robust process to ensure that they are able to quickly identify a breach.”

to safeguard its highest risk data appropriately, whether by way of security standards, access rights, or otherwise. While an organisation’s risk culture will vary depending on the nature of their data assets, employees at all levels should understand their role in keeping systems safe and secure. To this end, regular and up to date training is key, as well as an awareness of how cyber incidents may arise.

Q INSURANCE IS A KEY PART OF MANAGING CYBER RISK. HOW ARE INSURANCE PROVIDERS ADJUSTING OR ENHANCING THEIR INSURANCE SOLUTIONS TO MEET MARKET DEMANDS? WHAT TYPES OF POLICIES ARE AVAILABLE TO HELP MANAGE THE DOWNSIDE?

BAPAT: The type and extent of insurance coverage suitable for a company will vary according to the nature of a company’s data assets and its risk culture. The range of insurance products available in the market reflects this and companies need to be careful when selecting appropriate coverage. Coverage may be quite limited, such as ad hoc access to an advisory helpline service or, in the case of companies which hold large volumes of sensitive data, may be more extensive to include full access to key support such as legal assistance and full forensic IT analysis.

Q WHAT CONSIDERATIONS SHOULD COMPANIES MAKE WHEN EVALUATING CYBER INSURANCE COVERAGE, INCLUDING PRICING, POLICY PROVISIONS AND EXCLUSIONS?

BAPAT: The type of insurance coverage will vary according to the nature of a company’s data assets and its risk culture. While some companies may hold a vast amount of information, if this is not particularly sensitive they may not consider it cost effective to hold insurance coverage. Where companies do wish to insure against cyber risk, they should take care to ensure that the cover includes access to key support such as legal assistance or forensic IT analysis as required.
BAPAT: Cyber risk will continue to climb the boardroom agenda in the next year, in part due to the forthcoming General Data Protection Regulation which introduces a general data breach notification obligation on all companies suffering a data breach. Under the new law, coming into effect in May 2018, companies will have to notify a data breach to the relevant regulator within 72 hours. Where the data breach is likely to have a high risk of adversely affecting individuals, they too must be notified. There is no doubt that, in the future, companies will have to implement a robust process to ensure that they are able to quickly identify a breach as well as comply with the new notification requirements, not least to avoid the potentially large fines – up to €10m or 2 percent of annual worldwide turnover, whichever is greater.
Q HOW WOULD YOU SUMMARISE TODAY’S CYBER-RISK ENVIRONMENT? WHAT NEW RISKS HAVE EMerged IN THE PAST 12-18 MONTHS?

FRANÇOIS: The past 12 to 18 months have been marked by many changes in the cyber risk environment. Cyber attacks have increased in both number and sophistication. This has resulted in a higher number of data breaches, which often involve tens of millions of data. The French legislative framework has also evolved significantly, in particular with the implementation of the French Military Programming Law. That law obliges companies that have critical networks and information systems – so-called ‘operators of vital importance’ – to implement a cyber security mechanism. As a result, more than 200 operators have to comply with the security standards defined by the French National Cybersecurity Agency ANSSI, to implement strong detection mechanisms and to report major incidents to ANSSI. The first ministerial orders implementing these requirements came into force on 1 July 2016.

Q WHAT IMPACT HAS THE CLOUD HAD ON DATA SECURITY? WHAT SHOULD COMPANIES BE CONSIDERING WHEN TRANSFERRING DATA STORAGE TO THE CLOUD?

FRANÇOIS: The cloud may have security benefits, particularly for SMEs; it may offer them higher security levels than those that they can guarantee. On the other hand, the cloud generates new security risks, such as loss of governance, insecure or ineffective data deletion, excessive data retention or isolation failures, such as risks for data to be disclosed to unauthorised third parties and processed for illegitimate purposes. When transferring data storage to the cloud, companies should first consider the types of personal data that will be hosted in the cloud and the constraints related to this data. For example, in France, health data may only be hosted by a service provider approved by the French Ministry of Health. More generally, the French Data Protection Authority (CNIL) recommends that companies determine their own security requirements to ensure that the hosting service provider will meet all these requirements, and carry out a risk analysis to identify the appropriate security measures to be put in place. Companies should then consider the level of data protection offered by the service provider and choose a service provider that can implement such measures.
Q COULD YOU OUTLINE THE PRINCIPLES OF DATA PRIVACY LAWS IN FRANCE, 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?

FRANÇOIS: As outlined by the CNIL in its 2015 Annual Report, the concepts of cyber security and data protection are inseparable. Currently, the French Data Protection Act requires companies acting as data controllers to take all useful precautions with regard to the nature of the data and the risks of data processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by unauthorised third parties. In addition, the French Data Protection Act requires telecommunication service providers to report data breaches to the CNIL and individuals – when the breach is likely to adversely affect their personal data or privacy. The EU General Data Protection Regulation (GDPR), which will be directly applicable in the EU as from 25 May 2018, will extend these notification requirements to all businesses. It will also require businesses to take into account data protection issues when designing a processing system and during the processing (known as ‘privacy by design’), as well as to carry out privacy impact assessments (PIAs or DPIAs) for high risk processing. For most organisations, ensuring compliance with the new requirements could be quite a challenge.

Q WHAT STEPS SHOULD COMPANIES TAKE TO ESTABLISH APPROPRIATE PROCESSES AND POLICIES TO MANAGE CYBER RELATED RISKS? HOW IMPORTANT IS IT TO ADDRESS THE ORGANISATION’S RISK CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

FRANÇOIS: Companies’ first priority should be to have a good knowledge of their networks and information systems in order to identify the sensitive elements within the systems. This mapping exercise will be the first stage in risk analysis. Companies must be able to identify cyber risks to manage them. The risk analysis will lead to the definition of adequate technical and organisational security measures that should be formalised in an IT security policy. Among these security measures, protective barriers should be implemented such as physical access controls, network segregation, and so on. In addition, companies should implement detection mechanisms to be able to detect a security incident. Logs should be analysed regularly. These mechanisms should be accompanied by detailed response plans which are designed to handle the security incident and return to a normal
“It is crucial that organisations develop a cyber culture and consider cyber security in the initial stages of projects.”

situation as quickly as possible. In this respect, business continuity plans should take cyber security events into account. Companies should also keep themselves up to date by monitoring threats and vulnerabilities. Last but not least, companies should raise personnel awareness of cyber risks and carry out cyber security training programmes. It is crucial that organisations develop a cyber culture and consider cyber security in the initial stages of projects.

FRANÇOIS: Companies often do not have internal capabilities to manage cyber risks. To meet market demands, insurance providers are increasingly providing comprehensive insurance solutions, adding to their existing policies pre- and post-event assistance services. This typically includes risk assessment, crisis management and legal defence services. Insurance providers have been developing such solutions in collaboration with third-party vendors such as forensics investigators and consultants, to leverage costs and provide them at better rates.

FRANÇOIS: When evaluating cyber coverage, companies should consider the vulnerabilities of their networks and information systems, the means at their disposal to maintain system security at an acceptable level, legal, business or technical constraints, their internal capabilities to handle a cyber breach or data loss, the amount and type of personal data they are processing, threat developments, their risk appetite, and so on. The insurance policy should be tailored to each particular situation.
Q GOING FORWARD, MAJOR CYBER THREATS ARE ONLY LIKELY TO INCREASE. DO YOU BELIEVE CYBER RISK MANAGEMENT WILL CONTINUE TO CLIMB THE BOARDROOM AGENDA?

FRANÇOIS: Cyber risk management will definitely continue to climb on the boardroom agenda for several reasons. First, companies are increasingly reliant on IT technologies such as cloud computing, Big Data and connected objects, which increases their exposure to cyber attacks. Second, the costs of cyber attacks continue to increase. Third, breaches are more likely to be publicised, exposing companies to public opinion. Finally, the legislation becomes more stringent. For example, with respect to data security, the GDPR strengthens the obligations imposed on companies and significantly increases the level of sanctions – up to 2 percent of the company’s total worldwide annual turnover of the preceding financial year in case of non-compliance with the security obligations. This will certainly contribute to give higher priority to cyber security in boardroom discussions and hopefully to develop a cyber culture.

Claire François

Associate
Hunton & Williams
+32 2 643 58 00
cfrancois@hunton.com

Claire François is an associate in the Hunton & Williams Brussels office. Ms François is an associate in the firm’s European data protection and privacy practice, with an emphasis on French law. She advises clients on a variety of French and international data compliance projects, including implementation of global data management strategies, international data transfers (e.g., model contracts and binding corporate rules) and local data compliance. She also represents clients before the French data protection authority.
Q How would you summarise today’s cyber-risk environment? What new risks have emerged in the past 12-18 months?

SEGOVIA: Since the 1970s, progress in computing and telecommunications has transformed our lives. Today we talk about the IoT and Big Data; we are consolidating the idea of the ‘Smart Life’ in which we and the objects that surround us will be subjects of this new way of interacting with our environment. The rapid evolution of information and communication technologies has led to threats and attacks on infrastructure and other systems. These attacks are becoming increasingly numerous and sophisticated. Cyber space is becoming hostile, forcing us to employ increasingly innovative technical and human resources to cope. In recent months we have seen the speed with which ransomware attacks are increasing and how companies have no choice other than to pay ransoms quickly in order to restore their systems and services, or how social engineering techniques that seek to deceive employees to access what criminals want become highly successful. Security will move from being a capital investment model to be a continuous model – a process based on operating costs and outsourcing, alongside the provision for cyber insurance and risk management.

Q What impact has the cloud had on data security? What should companies be considering when transferring data storage to the cloud?

SEGOVIA: A growing trend among companies is to keep part of their data in the cloud as it is a convenient and economical system which can be accessed from any device and possibly saves space. However, comfort and security do not go together – usually the more comfortable a system is the less secure it is. Cloud storage creates interdependencies and clusters that arise from uncertainties in the real supply chain of providers, a lack of or lower control over such providers, and what happens to information services if a provider becomes insolvent. In this sense, companies will have to start being more aware, as well as more demanding or diligent in their knowledge of the supply chain.
SEGOVIA: In Spain we have an exacting legal framework regarding the protection of personal data: the Organic Law on Data Protection 15/1999 of 13 December. However, we must bear in mind that last April the new Data Protection regulation was approved in the European Union, the ascent of which demands new requirements, including data protection from design, security, notification of data breaches, promotion of codes of conduct and certification schemes, and so on. This does not necessarily imply a greater load but a different way of managing data protection. Some of the measures introduced by the new European regulation are a continuation of or replacement for existing ones. Others are formalising legal standard practices already implemented by companies, such as privacy by design, impact assessment and the appointment of a data protection officer. The main innovation introduced by this regulation is the obligation to notify. Under current legislation there is no such obligation, although it is a mitigating factor. This radically changes the scenario because companies are reluctant to do so due to reputational damage or punishment.

SEGOVIA: Cyber risk should be treated like any other risk. Companies should develop and promote key organisational capabilities to succeed in managing cyber risks, including the following three approaches. Firstly, risk analysis in order to prioritise assets that require greater protection. Secondly, necessary measures to ensure best practices in information security. And thirdly, preparing to detect and respond to cyber events through formalised organisational processes. Preparation in advance of any cyber incident will ensure that the initial problem is not made worse by avoidable errors that may be committed during response. Employees must know that they are part of this process, so they must be trained in cyber security based on their position within the organisation. A company should also have technical, qualified staff supported by professional
“Cyber risk insurance will continue to evolve to cover gaps in traditional insurance.”

services in cyber security. Being well prepared is essential to ensuring the organisation’s resilience.

SEGOVIA: Cyber risk insurance will continue to evolve to cover gaps in traditional insurance. A cyber attack can cause personal and property damage, and not only cyber risk insurance but traditional policies too, must develop to address such consequences. Although it is still incipient, the insurance market is starting to offer the first solutions based on policies acting as an umbrella for all risk and general liability insurance, so they are starting to cover property and personal damage arising from a cyber event in difference in conditions with such other policies. Apart from these new policies, interaction between traditional and cyber insurance should still be resolved. Likewise, insurance must prepare to meet the evolution of threats due to the IoT, Big Data, artificial intelligence and other factors, and develop new solutions. In the coming years we will see changes in the approach of some basic coverage of these policies, such as business interruption or liabilities.

SEGOVIA: The current offering of cyber insurance is broad and diverse, so it is important to ensure the adequacy of the offering matches the real needs of the organisation. Broad language for relevant definitions such as insured events, security failure or system failure should be sought. Organisations should ensure adequacy of coverage for contingent liability or dependent business interruption, as this may have a considerable impact on their business and continuity. In terms of provision, it is important to know if the organisation can resolve the cyber event with their preferred vendors as well as the extent of the offering of vendors by the insurer, and adapt or adopt the benefits of such offering within their internal event management. Regarding exclusions, try to remove war and terrorism exclusions or obtain affirmative coverage and establish appropriate carve backs for those losses arising from a breach linked to a known vulnerability that the insured was not able to address on time.
Q GOING FORWARD, MAJOR CYBER THREATS ARE ONLY LIKELY TO INCREASE. DO YOU BELIEVE CYBER RISK MANAGEMENT WILL CONTINUE TO CLIMB THE BOARDROOM AGENDA?

SEGOVIA: The new digital era is conditioned by a series of increasingly significant and difficult to control risks, and this makes companies and their managers increasingly vulnerable to them. A cyber attack can bring down the CEO, the alma mater of the company. We have already witnessed the resignations of Noel Biderman, founder and CEO of Ashley Madison, and Gregg Steinhafel, CEO of Target Corp, as recent examples. In this respect, managing cyber security has ceased to be a purely technical challenge; today it has become a strategic element of the business. Regulations are reinforcing this fact. For instance in Spain, the amendment of the Corporations Act establishes that the board of directors should decide the strategic aspects and control policies and risk management of the company, and that such decision is a non-delegable duty of the board. In fact, it is increasingly common for the chief information security officer to become part of the board.

Carmen Segovia Blázquez
Director Lineas Financieras Cataluña y Baleares
Aon Risk Solutions
+34 933 662 624
carmen.segoviab lazquez@aon.es

Carmen Segovia Blázquez is a director and national cyber leader at Aon Risk Solutions, with more than 10 years of experience analysing and providing insurance for risks related to financial and professional lines, as well as developing new coverages and strategies to face cyber risks. She participated in the analysis, development and placement of cyber insurance programmes for some of the main Spanish corporations of critical infrastructure, banking, industrial and retail sectors.
CHASTRE: The technological evolution and the wide use of the internet have contributed to the creation of the so-called ‘global village’. We have seen a number of changes to the social paradigm; new means of communication have emerged and have almost replaced the traditional physical and face-to-face means of social interaction. Although it is common knowledge that these new means of communication facilitate and promote a permanent and immediate interaction between the users, their use can be accompanied by some technological naivety which leads the users to share, sometimes without any type of restrictions, their personal data and in some cases the personal data of others. This ‘unrestrained sharing’ is mostly motivated by a false sense of security and not so much by the lack of technological training or information. The protection of data provided by users will be the key enabler of the future digital market. Only this way will users fully benefit from the digital economy, whether they are opening a bank account, joining a social network or purchasing book.

CHASTRE: The cloud has increased the difficulty of ensuring compliance with a number of legal provisions. One is keeping the data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Another is implementing the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subjects. Yet another is processing the data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing. A further issue is guarding against accidental loss, destruction or damage, using appropriate technical or organisational measures. Additionally, the current cloud computing business model is usually ‘one-size-fits-all’, meaning that the service provider does not know the nature of the data hosted by the service. Conducting a risk assessment and identifying the specific measures that are adapted to the category of data to be processed may cause
unexpected delays and costs. According to the new EU Regulation on Personal Data, a company choosing to process its data in the cloud will be required to select a service provider who can implement appropriate technical and organisational measures to meet the requirement of the data protection regulation and protect the rights of the individuals.

CHASTRE: First, data should be processed lawfully and with respect for the principle of good faith. Second, it should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. It should be adequate, relevant and not excessive in relation to the purposes for which it is collected and further processed. It should be accurate and, where necessary, kept up to date. Adequate measures must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which it was collected or processed, are erased or rectified. It should be kept in a form which permits identification of subjects for no longer than is necessary for the purposes for which it was collected or processed. It should be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Finally, legitimacy conditions, like obtaining the consent of the data subject, for example, should be met when processing personal data.

CHASTRE: To manage cyber related risks, companies should take into account the nature, scope, context and purposes of processing, as well as potential risks regarding the rights and freedoms of natural persons, before implementing appropriate technical and organisational measures to ensure and to demonstrate that processing is performed in accordance with applicable data privacy laws and regulations. Companies should also implement appropriate
IS IT TO ADDRESS THE ORGANISATION’S RISK CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

data protection policies specific to managing cyber related risks, and should adhere to approved codes of conduct or approved certification mechanisms that would enable them to benefit from the experience of other players in this field and to share their own experience and know-how. This is essential to managing and preventing cyber related risks.

CHASTRE: Cyber security insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches. Nevertheless, traditionally cyber security is not included in traditional commercial general liability and property insurance policies. Cyber security insurance is typically a ‘standalone’ line of coverage providing protection against data destruction or theft, extortion demands, hacking, denial of service attacks, crisis management activity related to data breaches, and legal claims for privacy violations. Few cyber security insurance policies offer businesses coverage for physical damage and bodily harm that could result from a successful cyber attack against critical infrastructure.

CHASTRE: Companies must take into account that cyber coverage is being most successfully used as a risk transfer option in those countries that have mandatory data breach notification laws. Companies must determine what costs or expenses they would like to have covered and what types of incidents they want cover for. Companies must also consider a range of questions. Which security controls can be implemented that will reduce the premium? What is expected of the company to reduce or limit the risks? Will the company be able to negotiate and receive a reduction for each year of not claiming? What assistance is provided by the insurer to improve information governance and information security? What support will be provided by the insurer to help make the right security decisions for the company? Can the insurer commit to updating the coverage to suit today’s fast changing cyber environment? Have all of the company’s portable devices been encrypted? Are malicious acts by employees covered? Will the company need to offer
"Companies must determine what costs or expenses they would like to have covered and what types of incidents they want covered for."

evidence of compliance to existing data protection principles to prove the right to be awarded? In those cases of uncertainty as to the nature of the incident, what is predicted by the policy? Are all and any court attendances to defend claims from others covered? Is the company able to claim if it was unable to detect an intrusion until several months or years have passed?

Q GOING FORWARD, MAJOR CYBER THREATS ARE ONLY LIKELY TO INCREASE. DO YOU BELIEVE CYBER RISK MANAGEMENT WILL CONTINUE TO CLIMB THE BOARDROOM AGENDA?

CHASTRE: The most recent reform of data protection rules in the EU proves, without doubt, that cyber risk management will continue to climb the boardroom agenda.

Cuatrecasas, Gonçalves Pereira

www.cuatrecasas.com

Leonor Chastre
Partner
Cuatrecasas, Gonçalves Pereira, RL
+351 21 355 38 12
leonor.chastre@cuatrecasas.com

Leonor Chastre is a partner who, since June 2013, has been in charge of the intellectual property, media and information technology department. Ms Chastre’s practice focuses primarily on arbitration, corporate and commercial, criminal law, intellectual and industrial property, media and data protection, pharmacy, health products and biotechnology (life sciences), and sports.
Q HOW WOULD YOU SUMMARISE TODAY’S CYBER-RISK ENVIRONMENT? WHAT NEW RISKS HAVE EMERGED IN THE PAST 12-18 MONTHS?

NAUWELAERTS: Multinationals, as well as SMEs, are faced with an increasing risk of cyber incidents that are constantly evolving and can take various forms, depending on the sector and industry. For example, with a growing number of transactions and personal data of customers being collected on a daily basis, online retail businesses are increasingly facing the risk of cyber attacks and other security related data incidents. The past year has also seen a number of cyber attacks targeting public sector institutions, including vital sectors such as nuclear energy and air transport. In order to help manage these risks, the federal government has supported the creation of a Centre for Cybersecurity. It is the first large-scale umbrella joint venture in the fight against cyber crime in Belgium, and serves as the main platform for collaboration and coordination with regard to cyber crime matters in Belgium, combining expertise of academic research groups, industry stakeholders and public organisations. The Centre organises and manages various projects on cyber security and assists with the preparation of cyber security standards and guidelines.

Q WHAT IMPACT HAS THE CLOUD HAD ON DATA SECURITY? WHAT SHOULD COMPANIES BE CONSIDERING WHEN TRANSFERRING DATA STORAGE TO THE CLOUD?

NAUWELAERTS: Using cloud services can increase the risk of data incidents, as cloud clients are typically no longer in exclusive control of data security and they are not in a position to deploy the technical and organisational measures that may be necessary to ensure the security of their data. In an opinion issued in February 2016, the Belgian Privacy Commission highlights this risk among several other risks associated with storing data in the cloud. The Belgian Privacy Commission recommends companies conduct a comprehensive and thorough risk analysis before moving data to the cloud, and carefully evaluate cloud service providers before engaging them. Cloud service providers should furnish prospective clients with all the information necessary to assess the pros and cons of their services. Security, transparency and legal certainty should be key drivers behind any offer from cloud service providers. In addition, appropriate contractual safeguards should be included.
in the service level agreement between the cloud service provider and its client; these safeguards should provide sufficient guarantees in terms of technical and organisational measures. Cloud service providers must also be able to guarantee the lawfulness of international data transfers if the clients’ data is stored outside of the EU/EEA.

**NAUWELAERTS:** In order to comply with Belgian data protection law, companies are required to implement appropriate technical and organisational measures to protect personal data from accidental or unauthorised destruction, accidental loss, alteration, access and any other unauthorised processing. These measures must also ensure the confidentiality and availability of the data. In addition to the implementation of data security measures, providers of publicly available electronic communications services in Belgium are obliged to notify both the Belgian Privacy Commission and any affected individuals of any data incidents. Although there is currently no general notification obligation, the Belgian Privacy Commission recommends notifying data breaches proactively and has issued specific guidelines in this regard. The guidelines include recommendations on how to prevent data incidents and when to report them. They are motivated by the Belgian Privacy Commission’s concern that companies often take their data security obligations too lightly, which increases the risk of security incidents.

**NAUWELAERTS:** Companies should take steps to prevent cyber related incidents to the fullest extent possible. These measures include performing data protection impact assessments to detect and evaluate possible risks and identify appropriate measures to mitigate those risks. Further, companies should have a documented incident response procedure that is duly communicated to their staff. The procedure should clearly identify
whom employees should contact, on a technical and management level, in the event of a data security breach, and should also clearly identify the relevant stakeholders’ roles and responsibilities. One of the major challenges for companies is to ensure that information about a cyber attack is communicated in a timely manner and to the right persons within the organisation. Therefore, educating employees about the available reporting mechanisms is key to managing cyber related risks. Further, companies should also consider preparing template communications that can be used to expeditiously inform the Belgian Privacy Commission – and, in some cases, affected individuals – in the event of a cyber incident.

**Q** INSURANCE IS A KEY PART OF MANAGING CYBER RISK. HOW ARE INSURANCE PROVIDERS ADJUSTING OR ENHANCING THEIR INSURANCE SOLUTIONS TO MEET MARKET DEMANDS? WHAT TYPES OF POLICIES ARE AVAILABLE TO HELP MANAGE THE DOWNSIDE?

**NAUWELAERTS.** More and more insurance providers in the EU are offering insurance solutions that cover a wide range of the risks, including risks associated with data breaches, business interruption and network damage. In some cases, they also provide coverage for the physical damage and bodily harm that could result from a successful cyber attack against critical infrastructure. Insurance providers are increasingly adapting their insurance strategies, tailoring solutions to the specificities of a company’s information systems and the risk culture within the company.

**Q** WHAT CONSIDERATIONS SHOULD COMPANIES MAKE WHEN EVALUATING CYBER INSURANCE COVERAGE, INCLUDING PRICING, POLICY PROVISIONS AND EXCLUSIONS?

**NAUWELAERTS:** Off-the-shelf solutions typically do not work in this context, and many companies prefer to negotiate bespoke cyber coverage. Also, it is expected that in the future an increasing number of companies will opt for cyber security insurance policies that ‘reward’ businesses for adopting and enforcing cyber security risk management plans – by providing more favourable rates. While major companies will mostly be in need of coverage dealing with the financial impacts of cyber attacks, many SMEs will also require advisory and technical support in the wake of a cyber attack.
“As cyber attacks become more aggressive and targeted, companies’ data security practices will have to be flexible and continuously adapted.”

Q GOING FORWARD, MAJOR CYBER THREATS ARE ONLY LIKELY TO INCREASE. DO YOU BELIEVE CYBER RISK MANAGEMENT WILL CONTINUE TO CLIMB THE BOARDROOM AGENDA?

NAUWELAERTS: Cyber security management will inevitably rise on the agenda of companies’ boards, because lack of compliance with the new data security requirements can potentially lead to administrative fines of up to 2 percent of total worldwide annual turnover in the preceding financial year. In the near future, companies will have to comply with data security obligations imposed by the GDPR, as well as the EU Network Information Security Directive (NIS Directive). The GDPR introduces a general data breach notification requirement applicable across all industry sectors, as well as an obligation to implement robust information security measures, apply privacy by design and run data protection impact assessments. We expect that these new legal requirements, combined with the increased risk of cyber incidents, will motivate more companies’ boards to start focusing on cyber security in the context of their company’s overall risk assessment and management. In addition, as cyber attacks become more aggressive and targeted, companies’ data security practices will have to be flexible and continuously adapted to face potential new forms of cyber attacks. This will require companies and their management to allocate an increasing amount of company resources to the prevention of cyber incidents. Last but not least, given that cyber attacks tend to attract media coverage, companies’ boards can no longer afford to give low priority to cyber risk management.

Wim Nauwelaerts
Partner
Hunton & Williams
+32 2 643 58 00
wnauwelaerts@hunton.com

Wim Nauwelaerts is a partner in the Hunton & Williams Brussels office. He heads the Brussels privacy and cyber security practice and is also the managing partner of the Hunton & Williams Brussels office. With more than 16 years of relevant experience, he advises and represents clients on all aspects of EU and international privacy and data protection law, including general compliance, data transfer strategies and representations before data protection authorities. He is recognised as a leading privacy practitioner by Chambers Global, Chambers Europe, The Legal 500 (Belgium), The International Who’s Who of Technology Lawyers and by Global Law Experts.
LEHMANN: Cyber risks are posing an ever greater threat to enterprises and the number of critical incidents is still rising. While the theft of data is a danger that has become common knowledge, new dangers are emerging, such as spear phishing. Emails and further communication are tailored to a specific person and his or her environment, so that the person is coaxed into believing that the correspondence is genuine. In the end, he or she acts in good faith that he or she is doing the right thing while actually damaging the enterprise. Another threat that has recently become prominent is the capturing of whole networks by criminals that only ‘release’ these networks after a ransom has been paid. Several hospital networks in Germany have fallen victim to those attacks, which could possibly endanger the lives of patients. Finally, attacks on physical infrastructure will become more numerous in the future. One example is a steel factory in Germany that suffered immense damage because its systems could not be shut down in a controlled way.

LEHMANN: The cloud has enhanced and mitigated the problem of data security. Enhanced, because every enterprise has to decide whether its data goes into the cloud and what security measures have to be taken both by the enterprise and the cloud-provider to keep the data safe. This is a rather demanding task for every enterprise that does not just want to sign a cloud computing agreement but wants to make sure that its data is as safe as possible. For a lot of enterprises, the security problem has also been made less complicated. Once the data is stored under the care of a reliable cloud-provider, it is very often safer than it was before. This applies, in particular, to smaller enterprises that would not have the means to establish sufficient technical security on their own.
Q COULD YOU OUTLINE THE PRINCIPLES OF DATA PRIVACY LAWS IN GERMANY, 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?

LEHMANN: Currently, with the GDPR becoming binding only in 2018, the most important source for data protection in Germany is the Federal Data Protection Act. Its basic principle is that the processing of data is prohibited until permitted by the data subject or by law. Consent by the data subject is only valid if given in an unequivocal way, voluntarily and on the basis of sufficient information. Every processing of data action – either on the grounds of the data subjects’ consent or on legal grounds – has to be appropriate and must not be excessive. The processing of data should be minimised from the start and every procedure should be structured in a way that minimises the data involved. These principles and their implementation are rather demanding because every processing action has to be carefully planned and constantly evaluated. Very often, businesses have to find a workaround or even to abstain from one way of processing because the law is a hurdle that cannot be overcome. As to security measures, these have to be appropriate and well documented.

Q WHAT STEPS SHOULD COMPANIES TAKE TO ESTABLISH APPROPRIATE PROCESSES AND POLICIES TO MANAGE CYBER RELATED RISKS? HOW IMPORTANT IS IT TO ADDRESS THE ORGANISATION’S RISK CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

LEHMANN: First of all, companies should evaluate their business processes and identify those parts of their activities that are critical because they either are dangerous or because the staff are acting in a way that is not focused sufficiently on security. That will show the status of the risk culture. Then internal or external experts should check what is necessary to become more secure. On that basis, it should be possible to find a way to make procedures safer by altering them and by making staff aware of possible threats or failures. Finally, one person should be made responsible for the implementation of new security schemes. This should be done via an official policy because documentation will be key under the GDPR and businesses should start now to prepare for the GDPR.
LEHMANN: Insurers are currently enhancing their services in some important ways. On the one hand, it is about to become a standard feature for premium policies that the security of the insured person’s IT has to be checked by external experts and retained by the insurer, first. Once the insurance contract has been signed, a lot of insurers provide preferred access to a team of emergency specialists, such as technicians, forensics and public relation experts. Within the context of such premium policies, coverage of up to €3m is readily available. On the other hand, insurers are establishing more and more standardised products, sometimes in connection with other policies, in order to make coverage affordable to small and medium-sized businesses. Cyber risk coverage may have been a rather sophisticated and individual coverage in the beginning – and still is with regard to premium policies – but now it is even available separately to general liability coverage.

LEHMANN: First, the company should choose an insurer that does not just calculate premiums and outline standard terms. It is important that the insurer offers an evaluation of the company’s security status first by external experts. That might not only serve to identify weaknesses but also to find a suitable basis on which to calculate premiums. The insurer should also offer access to an emergency team of experts, encompassing technical expertise as well as public relations and forensics. These experts must be available 24/7. The same applies to the insurer himself. As to the policy, that should be checked by an expert, with regard to the rest of the insurance coverage of the company, so as to avoid an overlap with other policies or a gap.
“Responsibility for security and for documentation no longer rests with the data protection officer but with the directors themselves.”

LEHMANN: Under the new GDPR, responsibility for security and for documentation no longer rests with the data protection officer but with the directors themselves. One particularly important new feature is the shift of the burden of proof to the company that now has to exonerate itself and show not only that it had all the security measures in place but also that it documented everything. If there were doubts about whether the measures were sufficient but the documentation was definitely insufficient, a company would be fined regardless. Given that these fines can now be up to €20m or 4 percent of the company’s global annual turnover, the directors must place compliance at the top of their list.

www.goerg.de

Dr Jochen Lehmann
Partner
GÖRG
+49 221 3366 0244
jlehmann@goerg.de

Dr Jochen Lehmann specialises in IT matters with a particular focus on data protection and data security matters. He is a member of GÖRG’s IT group, which is led by four partners including himself, as well as the firm’s internal IT advisory board.
Q HOW WOULD YOU SUMMARISE TODAY’S CYBER-RISK ENVIRONMENT? WHAT NEW RISKS HAVE EMERGED IN THE PAST 12-18 MONTHS?

OSGOOD: While point of sale software was very much the theme of 2015, latterly criminals have upped the ante and have set their sights on SWIFT, the world’s largest system for transferring funds between financial institutions. There has been an uptick in advanced persistent threats with a focus on compromising intellectual property from research & development institutions. Any country with a reputation for innovation is at risk and Australia is no exception, with the Australian Cyber Security Centre reporting that it sees cyber espionage activity targeting Australian networks on a daily basis. Finally, there has been an increase in malicious attacks directed at critical infrastructure. This is perhaps the most worrying trend given the impact a successful attack can have upon the wider population, as evidenced by the attack on the Ukrainian power grid earlier this year.

Q WHAT IMPACT HAS THE CLOUD HAD ON DATA SECURITY? WHAT SHOULD COMPANIES BE CONSIDERING WHEN TRANSFERRING DATA STORAGE TO THE CLOUD?

OSGOOD: The Australian Bureau of Statistics published its first report on the use of cloud services in July 2015 and found that the biggest roadblocks to adopting cloud technology were a lack of understanding of the services, closely followed by the risk of a security breach and uncertainty about where data may be located. Just as security can increase through the centralisation of data, it can also expose vulnerabilities due to the potential for volumes of data to be exploited through one targeted attack. The due diligence process for selecting a cloud service provider should be no less vigorous than that followed for any other key business decision. If companies are entrusting their most sensitive information to a third party, then security has to be front and centre, particularly given that in the event of a data breach it is highly unlikely that all responsibility will rest with the cloud service provider. Companies should ask about the disaster recovery plans of the cloud – how often are they tested and refined? What is their approach to threat intelligence and proactively hunting for vulnerabilities? Are controls implemented to segregate one company’s data from another?
OSGOOD: In April 2016, the Australian government released its cyber security strategy document committing to invest over $230m to bolster Australia’s defences over the next four years. This builds upon the earlier strategy document of 2009 which established CERT Australia, a national emergency response team and the focal point for the government in respect of cyber security related issues affecting major Australian businesses. On 12 March 2014, the long awaited update of the Privacy Act 1988 came into effect with a new set of unified principles named the Australian Privacy Principles. These principles currently govern how all private sector and not for profit organisations with an annual turnover of more than $3m must handle, store and manage personal information. The Privacy Act gives the Privacy Commissioner the power to investigate complaints and issue determinations which are enforceable by the Federal Court or the Federal Magistrates Court together with the ability to issue civil penalties in the case of serious or repeated breaches of up to $340,000 for individuals or $1.7m for a body corporate. The Privacy Commissioner’s preferred method of dealing with complaints is conciliatory — although many hoped he would use his enhanced powers to set an example of companies failing to meet the required standard. Since 2010, the Privacy Commissioner has issued 12 determinations, with the maximum penalty issued to date being $15,000.

OSGOOD: irrespective of how much a company invests in protecting itself against cyber related risks, it is only as strong as its weakest link, and it is becoming increasingly apparent that ‘human risk’ present a significant threat. Spear phishing campaigns targeting employees increased by 55 percent in 2015. If a company is not promoting a culture of IT security awareness then employees will be unaware of the threat environment, and the likelihood of an attack against their company being successful will increase. Aside from educating employees, it is crucial for companies to regularly scan their
"If the past is an indicator of the future, the threats are only going to grow in complexity and severity."
Osgood: Cyber threats are not going away any time soon, and if the past is an indicator of the future, the threats are only going to grow in complexity and severity. Board members have a fiduciary duty to safeguard the assets of their company and cannot afford to turn a blind eye to cyber risk. We have seen executive management being held accountable for many high profile breaches in recent years, including Target and Sony, which reinforces the notion that board management and executives need to play a pivotal role in ensuring that cyber security is made an enterprise-wide priority and that their company is well placed to respond to threats before, during and after a breach occurs.
GOTTSCHALK: The financial services industry, among other sectors, continues to be a target for cyber attack and this is largely due to the potential financial rewards on offer for the attacker. Ransomware remains a prevalent burden and continues to show how effective it can be in its ability to disrupt business operations. Most recently we have seen cyber attacks using advanced malware with the ability to bypass key controls. While this not in itself groundbreaking, we are starting to see these attacks being more and more successful against organisations, where their environments are considered very mature.

GOTTSCHALK: The common concern relating to the cloud is where one's data is actually being stored, from a jurisdiction perspective. A typical example would be: if your organisation resides in South Africa and its data is being stored by the cloud provider in the US, then your data cloud may be subject to the laws of that country. This may result in your data being accessed by a third party without your permission. Organisations should be more concerned with gaining comfort around the security controls that the cloud provider has put in place in an effort to safeguard their data. This may include controls that ensure adequate segregation from potential competitor data, reducing the risk of unauthorised access.
GOTTSCHALK: Within South Africa, the Protection of Personal Information Act (POPI) stipulates eight guiding principles which organisations must adhere to. As the regulator is yet to be established, breach notification processes will still need to be established, as well as further guidance around the implementation of security measures that are considered leading practice. This may take the form of the regulator driving compliance with leading practice standards such as ISO 27001. The key principles of the POPI Act require the organisation to have an accountable person who will ensure that the responsibilities of the Act are met. Furthermore, the organisation will be responsible for its security safeguards, as well as the safeguards of its third parties.

GOTTSCHALK: Security awareness training is frequently neglected, however, it is a vital component in the fight against cyber attacks. By driving security awareness within an organisation, you are slowly changing the culture around security by enabling people. This is achieved by making them aware of how they may be targeted, as well as giving them the skills they need to identify and respond to a successful social engineering attack.
Q INSURANCE IS A KEY PART OF MANAGING CYBER RISK. HOW ARE INSURANCE PROVIDERS ADJUSTING OR ENHANCING THEIR INSURANCE SOLUTIONS TO MEET MARKET DEMANDS? WHAT TYPES OF POLICIES ARE AVAILABLE TO HELP MANAGE THE DOWNSIDE?

GOTTSCHALK: Within the South African market, cyber insurance is fairly new, though the interest and uptake is certainly high. The key challenge with cyber insurance is ensuring that organisations are adequately insured and that the insurer is comfortable with the organisation’s level of security controls, which will result in non-repudiation of claims. In the event of a breach, organisations have the responsibility of proving the occurrence of the breach/attack to the insurer, which has subsequently resulted in a loss for the organisation. The ability to do so will require the organisation to have adequate monitoring in place to manage this requirement. Depending on the insurer, cyber insurance policies often fall into two categories: first-party or third-party coverage. First-party coverage offers financial compensation that aids organisations in addressing immediate customer and business needs. Third-party coverage typically addresses the financial risk brought upon an organisation through litigation by customers or third parties. Aspects of each of these coverage areas can be combined.

Q WHAT CONSIDERATIONS SHOULD COMPANIES MAKE WHEN EVALUATING CYBER INSURANCE COVERAGE, INCLUDING PRICING, POLICY PROVISIONS AND EXCLUSIONS?

GOTTSCHALK: Purchasing cyber insurance requires careful consideration and negotiation of the policy language to ensure that your company is purchasing the right coverage. As with other insurance policies, cyber policies contain a host of exclusions and limitations to coverage. One can obtain enhancements eliminating or limiting the scope of certain exclusions for little or no additional premium. There are specific policy terms and conditions to consider when evaluating a cyber insurance policy, which may include the following: first, cyber policies often restrict coverage to breaches or losses that occur after a specific date, and in some forms, it is the inception date of the policy. While breaches may go undetected for some period of time, it is important to purchase coverage with the earliest possible retroactive date. Second, companies should make sure that data stored with third parties or in the cloud is covered, even if the third party experiences the data security breach. Finally, sublimits can greatly reduce coverage. Most cyber insurance policies impose sublimits on coverage, such as notification costs and regulatory investigations. These sublimits are often inadequate.
"The change that is required is the acknowledgement from business that cyber is a business responsibility as much as an IT responsibility."

Q GOING FORWARD, MAJOR CYBER THREATS ARE ONLY LIKELY TO INCREASE. DO YOU BELIEVE CYBER RISK MANAGEMENT WILL CONTINUE TO CLIMB THE BOARDROOM AGENDA?

GOTTSCHALK: Boardroom agendas are usually filled with discussions around cyber. The change that is required is the acknowledgement from business that cyber is a business responsibility as much as an IT responsibility. Business needs to be part of the solution and drive the identification of critical business assets and prioritisation of spend to protect these assets. This should be achieved through joint responsibility between business and IT. A key aspect of cyber risk management will be around crisis management and ensuring that the organisation is prepared to respond in a cohesive manner.

Jason Gottschalk
Associate Director
KPMG Services (Pty) Ltd.
+27 8 2719 1804
jason.gottschalk@kpmg.co.za

Jason Gottschalk is an Associate Director at KPMG, and the driving force behind KPMG’s innovative cyber security services within the South African market. Having grown up in the age of pioneering technologists, Mr Gottschalk has 16 years of coal-face experience under his belt. His hands-on knowledge of networks and systems security, academic research in Industrial Control System security and his breadth of industry insights and war-stories have led him to be a trusted adviser to KPMG’s national client base, and a recognised personality in the world of cyber security.
Target’s Directors and Officers Dismissed from Data Breach Lawsuit

Target Corporation’s (Target) directors and executive officers can breathe a sigh of relief after a Minnesota federal judge dismissed derivative claims brought against them by Target shareholders, stemming from a data breach in 2013 in which hackers stole credit card and other personal information of tens of millions of Target customers. Davis v. Steinhafel, No 14-cv-00203 (D. Minn.). This decision provides useful guidance for directors and officers on the issues a court may consider in determining whether to allow a derivative suit to proceed based on alleged violations of fiduciary duties in overseeing corporate cybersecurity.

The Breach

On December 19, 2013, Target disclosed that hackers had breached its online systems and stolen payment card data from up to 40 million consumer credit and debit cards used in Target stores from November 27 to December 18, 2013. On January 10, 2014, the company divulged that personally identifiable information—such as names, mailing addresses, phone numbers, and email addresses—of up to 70 million more customers was stolen during the breach. The attack brought widespread media attention, negatively affected Target’s sales and reputation, and subjected the company to lawsuits by banks for their costs in reinstating consumer credit cards.

The Derivative Litigation

Following the breach, Target shareholders filed derivative actions in Minnesota—one in state court and four in federal court—against Target directors and certain executive officers. The federal cases were consolidated and the state lawsuit was stayed pending the outcome of the federal case. The shareholders alleged that the defendants breached their fiduciary duties by failing to properly provide for and oversee an information security program, by actively attempting to conceal the extent of the breach, and by failing to give customers and the public prompt and accurate information about the breach. Pursuant to applicable Minnesota law, Target formed a Special Litigation Committee (SLC), comprised of disinterested and independent directors (two former judges appointed to the board solely for this purpose) to investigate the claims and determine whether it would be in the best interests of the company to pursue the litigation.

Review by the SLC

After a lengthy and extensive investigation that included reviewing thousands of documents related to Target’s information security and procedure, performing dozens of interviews, consulting with experts, listening to presentations from the shareholders’ counsel, the directors’ counsel, and Target’s counsel, and reviewing applicable law, the SLC concluded it was not in Target’s best interest to pursue the litigation against the directors and executives.

Under Minnesota law, a court will defer to an SLC’s recommendation to dismiss a derivative action so long as: (1) the SLC was comprised of disinterested and independent members; and (2) the SLC’s recommendation is based on a good-faith investigation of the
allegations. Based on its investigation, the SLC filed a motion to dismiss the lawsuit. Target, its officers, and directors likewise filed three separate motions to dismiss. The court granted their motions and dismissed the action.

**Take-Aways for Directors and Officers**

Directors and officers can look to the Target SLC report as a guidepost for the types of measures that should be a part of a robust information security program to help establish that they have discharged their fiduciary duties. Factors that the SLC reviewed, considered, and relied upon included:

- The existence of network-security insurance that mitigated the cost of the breach.
- Pre-breach policies and procedures that incorporated technical, administrative, and physical controls for data security.
- Pre-breach vendor security procedures.
- Employee training related to data security requirements.

While future courts will review derivative actions on a case-by-case basis, the Target defendants’ situation illustrates the importance of being able to demonstrate a strong, even if imperfect, cybersecurity program. The more evidence directors can produce to demonstrate that they prioritize and enforce cybersecurity, the more difficult it will be for plaintiffs to sustain breach of fiduciary duty claims against them following a breach.