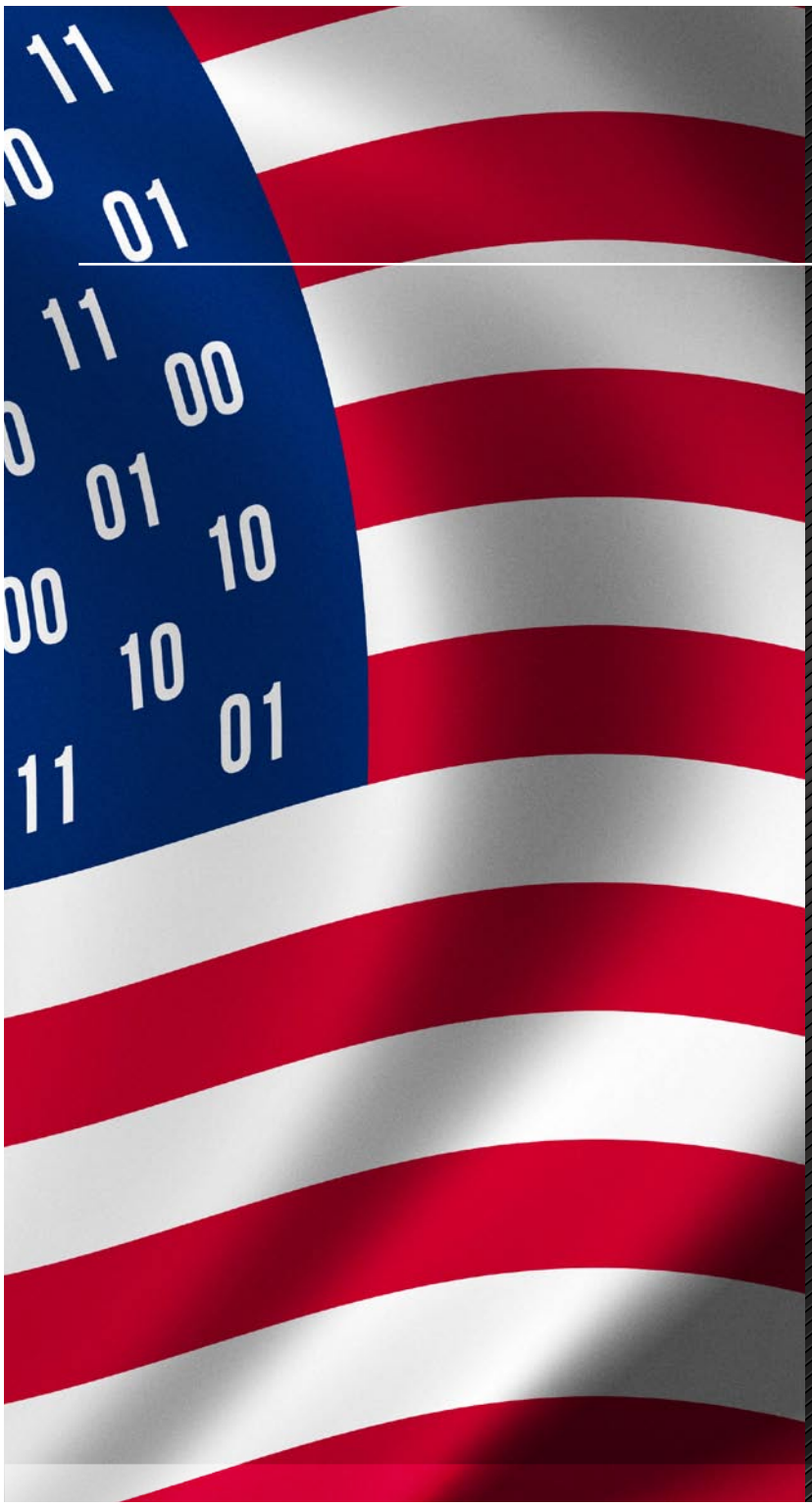
REPRINT

FINANCIERWORLDWIDE.COM

PREPARED ON BEHALF OF

Kroll



TalkingPoint

D&O LIABILITY IN DATA PRIVACY AND CYBER SECURITY SITUATIONS IN THE US

REPRINTED FROM EXCLUSIVE ONLINE CONTENT PUBLISHED IN:

JANUARY 2014

FINANCIER WORLDWIDE corporatefinanceintelligence

FW moderates a discussion on D&O liability in data privacy and cyber security situations between Richard Bortnick, a shareholder at Christie, Pabarue and Young, Jonathan Fairtlough, a managing director at Kroll, and Ann Longmore, an executive vice president at Willis.

Richard Bortnick
Shareholder

Christie, Pabarue and Young

Richard Bortnick is a shareholder at Christie, Pabarue and Young. Mr Bortnick litigates and counsels US and international clients on cyber and technology risks, exposures and best practices, directors' and officers' liability, and commercial litigation matters. He is Publisher of the highly-regarded cyber industry blog, Cyberinquirer.com and is an internationally recognised lecturer with an extensive list of presentations across North America, Europe and Asia. He is licensed to practice before the US Supreme Court as well as all courts in Pennsylvania, New York and New Jersey. Mr Bortnick can be contacted on +1 215 587 1688 or email: rbortnick@cpmy.com.

Jonathan Fairtlough
Managing Director

Kroll

Jonathan Fairtlough is a managing director with Kroll's Cyber Investigations Practice, based in Los Angeles. Mr Fairtlough joined Kroll after a distinguished career with the Los Angeles County District Attorney's Office where he served as both a prosecutor and co-founder of the office's High Technology Division. During his career Mr Fairtlough has held a number of positions within the District Attorney's office and has been involved on many high profile cases, including the first major data breach filed in Los Angeles County. At Kroll, he leads assignments providing comprehensive investigative services for digital forensics, data breach response, and complex cyber-crimes. He can be contacted on +1 213 443 1121 or by email: jfairtlough@kroll.com.

Ann Longmore
Executive Vice President

Willis

Ann Longmore is an executive vice president at Willis' FINEX North America division. Ms Longmore brings a combination of educational and business credentials to her work on issues concerning liability and insurance relating to Directors & Officers, (Pension) Fiduciary and Employment Practices exposures. Prior to joining Willis, she spent 10 years at a large multinational insurance company, where she oversaw risks relating to corporate, not-for-profit, multiemployer and public plans. Her previous legal experience includes positions at the New York Stock Exchange and the Bankruptcy Court in New York's Eastern District. Ms Longmore can be contacted on +1 212 915 7994 or by email: ann.longmore@willis.com.

FW: In your opinion, what are the key risks to D&Os arising from data and security breaches in the United States? Could you outline any recent 'cyber liability' cases of note?

Bortnick: Like other entrepreneurs, lawyers are typically on the look-out for the next big thing, economically speaking. You can count American securities fraud lawyers among these entrepreneurs. For many years, they prosecuted cases involving alleged accounting fraud. Then LIBOR became a significant source of litigation and the real estate bubble burst. Logically, it would seem that cyber- and technology-related risks and exposures are in plaintiffs' lawyers' sights. Best practices filter throughout an organisation from the top down. If D&Os ignore or even fail to account for the gravity of cyber, technology, and privacy risks and exposures, they are setting themselves up to be sued. The costs of a proactive loss avoidance and remediation strategy can be dwarfed by the response costs for those companies that haven't created, implemented and properly tested such an approach. It should be a no-brainer. Sadly, it's not. Which, of course, is music to the ears of lawyers, both plaintiff and defence.

Fairtlough: Leaders that fail to address cyber threats risk loss of income, loss of business reputation, and potentially loss of their position. Regulators and investors will hold management accountable for poor risk management. Look at the reality in just one field – healthcare. The Office of Civil Rights for Department of Health and Human Services has received over 85,000 complaints of HIPAA privacy violations this year. Of these, 30,000 required corrective action and 518 have been referred for criminal prosecution. The breaches compromised the data of over 28 million people. In August, Affinity Health Plan settled for $1.2m over failure to wipe copier data exposing 533,000 records. If your entity creates, receives, maintains or transmits PHI on behalf of a covered entity, HIPAA now governs your business.

Longmore: Cyber data and security breaches, if they are material to the firm and the business of the organisation, can result in D&O claims brought by shareholders and potentially regulators. Notably examples of shareholder actions include Heartland Payment Systems – an early shareholders' securities class action brought back in 2008 following a stock drop after the disclosure of a significant data breach. The case was dismissed due to the plaintiff's failure to sufficiently allege that the company had made false or misleading statements relating to its data security. Importantly, this decision pre-dates the US SEC's cyber disclosure guidance, suggesting that outcome of such a case might be different. In TJX Companies, Inc., shareholders brought a derivative suit following a significant data breach. The case settled back in 2010.

FW: What steps can D&Os take to prevent data breaches and cyber intrusion? What are the particular challenges and costs associated with mitigating these risks?

Fairtlough: Executives need to understand that perimeter cyber security can be strong, and breaches will still happen. A strong IT defence is still needed, but to achieve meaningful risk-based protection, businesses need to move from a 'boundary-based' mentality to the more nuanced and realistic viewpoint of 'defence in depth'. A company should institute additional controls and monitoring mechanisms to recognise intruder activity within systems, and to record what intruders do in the system. Track access to the crown jewels of corporate data. Examine workflow and policies to ensure that monitoring systems are geared to review the actions of employees, contractors, temporary workers, vendors or other third parties. The costs for

risk mitigation are soft – they involve tasking monitoring responsibilities properly, ensuring regular training, and constantly reviewing data security policies.

Longmore: In today's world, we have recognised that it is a matter of 'when' and not 'if' when it comes to cyber intrusions for most firms. To determine what preventative measures are best for an organisation, D&Os must first have an understanding of the challenges facing the institution. Fortunately, the National Institute of Standards and Technology (NIST) has begun to release its Preliminary Cybersecurity Framework to assist in understanding and reducing cyber security risks. Beginning with critical infrastructure – such as technology, telecommunications, finance, healthcare, transportation and the like – the NIST framework will include standards, guidelines, and best practices to promote the protection of critical infrastructure. The prioritised, flexible, repeatable, and cost-effective approach of the framework will help the board understand and participate in decision making as respects cyber security. Importantly, we expect the framework to facilitate board understanding and discussions of these risks in a robust manner not previously achievable.

Bortnick: In a nutshell, develop, implement and regularly update cyber security best practices. As such, it is imperative to spend capital up front to avoid the severe – and potential company threatening – negative impact of a cyber incident. At the outset, companies should look to attorneys who carry the attorney-client privilege to assist in creating and implementing a best practices-driven cyber incident avoidance and response plan on a company-wide basis. Virtually all entities, large and small, maintain clients', customers' and employees' personally identifiable information, financial information and, in some cases, personal health information. And every such entity is a cyber incident away from losing their clients', customers' and employees trust – and business. Perhaps most importantly to a company's senior management, the institution of a strong, company-wide cyber risk management program will cost a fraction of the expense and repercussions of a cyber incident. In other words, you can pay me now or pay me later. And if it is later, a company may have far bigger problems than trying to simply put the horse back in the barn.

FW: What legal and regulatory issues are affecting the ways companies manage data and approach cyber security? How constructive, in your opinion, is government guidance regarding cyber security risks and cyber incidents across the US?

Longmore: The question as to whether or not cyber security breaches could lead to the next big wave of D&O securities litigation has undoubtedly gained more traction due to the SEC's disclosure guidance to public companies. On a state basis, the various breach notification requirements now in place – and evolving – have led to important changes in data handling, breach response and cyber insurance. One only has to review the conclusions and follow-on suggestions in the California Data Breach Report 2012 from the State's Attorney General to see this in action.

Bortnick: From a macro-level, government oversight is not a bad thing. Many companies are reluctant to invest the resources to initiate a best practices regime. The problem is that in the US, there is no uniform legislation or regulatory mandate concerning cyber security and breach notification to affected persons and regulators. The federal government has failed to institute omnibus cyber security legislation, instead relying on a hodgepodge of sector specific rules and regulations governing classes such as critical infrastructure, health care, financial institutions and other demographics. As such, regulatory oversight has been relegated to the states, 46 of which – as well as the District of Columbia

and other US territories – have enacted sometimes inconsistent rules and requirements that are frequently confusing and expensive to navigate. Whether one fancies or doesn't fancy government supervision, it exists on a fractured basis. Administrative control is here to stay. At the very least, there should be consistency and uniformity so that companies know and can properly operate in accordance with one set of rules.

Fairtlough: Cyber security and data management is becoming a legal compliance nightmare. Depending on the type of data a company holds, there are different legal and regulatory issues. Protected Health Information (PHI) is regulated by HIPAA/HITECH. Financial information is regulated by several different statutes. Personally Identifiable Information (PII) is regulated on a state by state basis. Payment Card Information is regulated via the PCI-DSS agreements with credit issuers. Educational records and student data is regulated by FERPA. Different nations handle data protection laws differently. On top of this framework of patchwork regulation and differing definitions, the National Institute of Standards and Training has just issued the Preliminary Cybersecurity Framework. These statutes can provide guidelines for compliance, but too often, the regulations encourage compliance with the rules, not a thorough security evaluation. A prudent manager does not confuse compliance with meaningful security. Cyber security and data management policies must be regularly checked to ensure real security compliance.

FW: How should firms in the US respond when they fall victim to cyber-crime? What immediate steps should D&Os take in the early phase following such an occurrence, such as conducting an internal investigation?

Bortnick: Before you know how to manage a problem, you first must understand what the problem is. Was there a significant event or a relatively minor hiccup? Who and what are impacted? What is the economic, social and societal effect, if any? These inquires, and a well-thought, technically sound strategy, can and should be made promptly and decisively. One does not need to know how bad something might be. But whether a cyber incident is big or small, and regardless of the precise empirical and social impact, every company should and can have an appropriate and effective incident response plan. In other words, a company should be well positioned to promptly determine what it is dealing with, how it happened, and how to avoid, if not prevent, a cyber incident from occurring or reoccurring. For example, has the company instituted a best practices regime on both the front-end and back-end of its approach to cyber incident avoidance and remediation. If there has been a breach, should the company get the FBI and other government officials involved in the investigation and incident response plan? Is there dedicated cyber insurance in place that will cover some or all of the fallout of a cyber incident, from crisis management to business interruption expense to reputational impact? If so, has someone timely notified the underwriter to eliminate any issues regarding the timeliness and propriety of reporting? What crisis management vendors' services are needed, if any? Do you notify affected persons? In short, the questions are not hard to identify. The devil is in the answers.

Fairtlough: Call for help, and halt. Few organisations have the personnel trained in cyber investigations for the appropriate handling of data in an investigation. We've seen cases where IT personnel trying to respond an incident end up either destroying information entirely or tainting it in a way that ruins its evidential value. The insider threat is always an issue. What happens when an in-house 'investigator' turns out to be implicated in the incident, either as a participant or by having

ignored or allowed a security gap which permitted the incident? Pre-identify and establish a relationship with a cyber investigation team. Vet the organisation to ensure that it holds the proper licenses to do the work. This is especially important where D&Os have had the foresight to put a cyber insurance policy in place. Allowing untrained personnel to investigate incidents can result in incorrect conclusions and claims of bias in a dispute. Many carriers have already vetted and negotiated with approved vendors.

Longmore: It is absolutely critical, before a data breach occurs, is for firms and their boards to review their cyber incident response plan and consider engaging in a desktop simulation of a serious hack. The plan and the simulation might take the board and key individuals at the organisation through the immediate event as it unfolds, and then look at the necessary action steps over a period of time. This might best be done in concert with the forensic firm that the organisation proposes to conduct the resulting investigation and other relevant third parties. May I suggest that one's insurance experts also participate to consider and include the critical role that insurance coverage might play in such an instance?

FW: What insurance solutions exist for D&Os, in connection to cyber security and data breaches? How aware are D&Os of the existence and the availability of risk transfer options?

Fairtlough: Clear, unambiguous cyber coverage for a D&O policy is necessary. Directors should know what the corporation is doing to prepare and protect against cyber events. Directors should be talking to their risk managers about insurance solutions – solutions that facilitate not only the response but preparedness as well. From an E&O perspective, cyber insurance can cover both first and third-party claims, but from a D&O perspective, there will be an increasingly visible need to protect the board and the organisation from allegations that they failed to provide proper oversight to prevent cyber attacks. While this customised risk-transfer solution exists for the D&O market, it is critical that it is utilised. Even in the procurement of traditional D&O policies, the board may be asked about cyber preparedness in insurance applications. As the nexus between cyber events and shareholder derivative suits continues to strengthen, brokers and counsel may want to advise clients about the availability of cyber insurance products in the marketplace.

Longmore: A number of cyber insurance solutions exist – for firms of all sizes and industry groups. These range from cyber insurance itself to extensions to one's professional liability (E&O) insurance, to D&O coverage, to potential coverage under a Fidelity bond or Kidnap and Ransom insurance. Understanding the possible overlaps and gaps is critical to determining the best solution for the D&Os and the organisation. Sadly, in reviewing public company security disclosures relevant to cyber risks, where the SEC had suggested that information as to insurance might be included as part of the discussion on preventative measures, we found that most companies did not disclose or appear to fully understand what insurance existed.

Bortnick: Sadly, cyber insurance remains a generally unknown and misunderstood product. Outside of a small, but growing, number of retail insurance brokers who are educating their clients about cyber risks and exposures and the available risk transfer mechanisms, the retail broker community is not properly counseling their public, or private, company executives of the need for, and benefit of, dedicated, standalone cyber insurance coverage and the need for best practices. Put another way, the coverage afforded by a D&O insurance policy has been drilled into every directors' and officer's

head for over 25 years. In some cases even longer. What many senior executives don't yet appreciate is that while a D&O policy might cover a securities-related or corporate governance lawsuit, it won't cover most or all of the expense resulting from a cyber incident. They must be educated about the risks, exposures and solutions, including insurance, before it is too late. And too late could be tomorrow.

FW: What can companies do to reduce their risk and ideally reduce their rates prior to obtaining a cyber-liability policy?

Longmore: All cyber insurance carriers have their own lengthy applications for cyber insurance, seeking to address the source and size of the firm's potential exposure as well as the organisations security technologies. Overall, vulnerabilities may be dependent on one's industry sector, which cannot be changed, but one's risk profile can be improved by demonstrating that one meets or exceeds sector-specific industrial control systems and mitigation strategies. Similarly, we are all dependent to some extent on vendors. Demonstrating diligence in assessing, controlling and containing vendor-related cyber risk is the next critical link established by superior cyber risks.

Fairtlough: Underwriters in this field are specialists and have a strong technical comprehension of the risks involved. If a company is able to show that they put measures in place during the ordinary course of business, it will become a more attractive risk to the carrier. Some carriers offer cyber readiness programs and prospective insureds that may otherwise be denied coverage may receive a second review if they participate in a readiness program and show measurable improvements. Some carriers have built in incentives to promote readiness; if a company is subject to an attack but can prove they did everything proper and reasonable to prepare, they most likely will not be affected as severely upon renewal had they not show proactive efforts.

FW: What are the benefits of maintaining a pre-existing relationship with vendors on a cyber liability policy list of providers?

Fairtlough: Maintaining a pre-existing relationship with vendors has several advantages. First, carriers that develop panels typically spend a lot of time and dedicated resources doing the due diligence on the vendor's expertise and reputation, and oftentimes negotiate discounted rates. Panel vendors are also aware of the tripartite relationship between the carrier, the insured and outside counsel and can integrate with the team seamlessly. The teamwork facilitates ease of communication, assists in the reporting process and can even streamline the business process. There is also an advantage to working with one vendor repeatedly. The vendor begins to know the companies' systems, key management figures and outside counsel, which can save time and money in the long run. Consistency and repeatability in process can also provide the groundwork for defensibility in any argument, should a cyber event occur despite best efforts.

Longmore: A pre-existing relationship with a cyber response firm is a clear advantage when it comes to designing and implementing the critical incident response plan, potentially reducing the organisation's downtime while also improving the communications phase involving regulators, customers and other stakeholders. Including these on your insurance carrier's pre-approved vendor list means that the path to insurance coverage for these activities is also cleared and ready for payment.

Bortnick: Cost is the driving factor. As noted, it is far cheaper to put an effective risk management plan

into practice before a cyber incident occurs than have to respond on an ad hoc basis once an event has occurred. Equally important, a proactive approach enables companies to delegate their risk management and response regimes to experienced, trusted advisers and service providers. Of course, this also translates to the bottom line, as a self-guided plan could cause a tremendous economic impact in terms of lost opportunity costs. A company should leave it to their trusted experts to avoid and manage a cyber incident and only get involved as needed. That way, they can focus on what they enjoy and do best: operating their core business.

FW: What are your predictions for the cyber security landscape over the next 12-18 months? Do you expect any further regulatory or legislative changes, and what will be the impact on D&Os?

Longmore: In the US, there is a call for the SEC to further enhance its existing cyber exposure disclosure guidance, and the NIST framework for critical infrastructure organisations is still in the comment stage. Importantly, neither of these important initiatives is overtly compulsory or prescriptive in nature – indicating that the regulators would rather use a 'carrot' than a 'stick' at the current time. On the state level, we expect to see a continued evolution of breach notification rules, likely expanding them to include additional information and refining the definition of Personally Identifiable Information (PII). Federal legislation of this area would resolve inconsistencies, but is not likely to pass in the next year, year and a half. On the global stage, the US and European authorities are quietly cooperating on modifying the patchwork of existing regulations. While the bar for breach disclosure requirements may be raised in the EU, avoidance of competing provision is likely to reduce the complexity of compliance for organisations.

Bortnick: The number of cyber related incidents will continue to grow both in terms of frequency and severity. So too, the root causes of cyber related incidents will continue to evolve. BYOD, Social Media, on-line banking and shopping, medical records stored by health care providers and vendors – how many people would have imagined that they would be worried about such risks in 2013? Much less in 2003, by which time cyber privacy insurance already was being offered by a number of forward-looking insurance markets that understood that the world economy was migrating to a virtual platform. The use of technology will only grow – exponentially. And so too will the resulting cyber risks and exposures. The insurance market has been growing 20-30 percent annually. Name another sector whose revenues are increasing at that rate, particularly in a slow global economy. There will be countless cyber-related incidents in 2014 and beyond. And prudent companies cannot 'ostrich' and pretend they won't be on the growing list of victims. They should not and cannot play games with their businesses' economic vitality and continuity, whether from an operational or infrastructure perspective. In terms of proactive government action, very little will happen federally beyond the already heavily regulated critical infrastructure, healthcare and financial sectors. For now, the federal government is focusing on critical infrastructure as the associated risks there threaten the Homeland. Next will come the financial sectors, which already have some level of oversight based on Graham-Leach Bliley and the SEC Cyber Guidance, among other sector-specific laws. On the other hand, state legislators and regulators will continue to expand companies' duties and obligations to the extent they impact constituents. Americans value their privacy and the privacy of their personal information – and elected officials value their jobs. Until the federal government enacts uniform national legislation, protection of citizens' privacy will rest with the individual states.

Fairtlough: Companies and insurers should expect an increased volume of regulatory and legislative changes that require holders of key sets of data to protect that data or risk liability. This is particularly true for companies that operate internationally. The European Union is looking at updating the EU Privacy Directive, to strengthen controls. Further, there is a faction in the European Parliament with a group of members (MEPs) who purport that the current structure of the agreement permitting the flow of PII between the EU and US is fundamentally flawed, and does not provide sufficient security to serve as the basis for authorised data transmissions. Other nations are also moving in the direction of greater control and adoption of a more EU-like set of privacy principals and rights of data subjects. At home, the release of the new proposed cyber security framework and the patchwork of regulatory compliance make a strong risk-based data defence key to successful business operations. ■