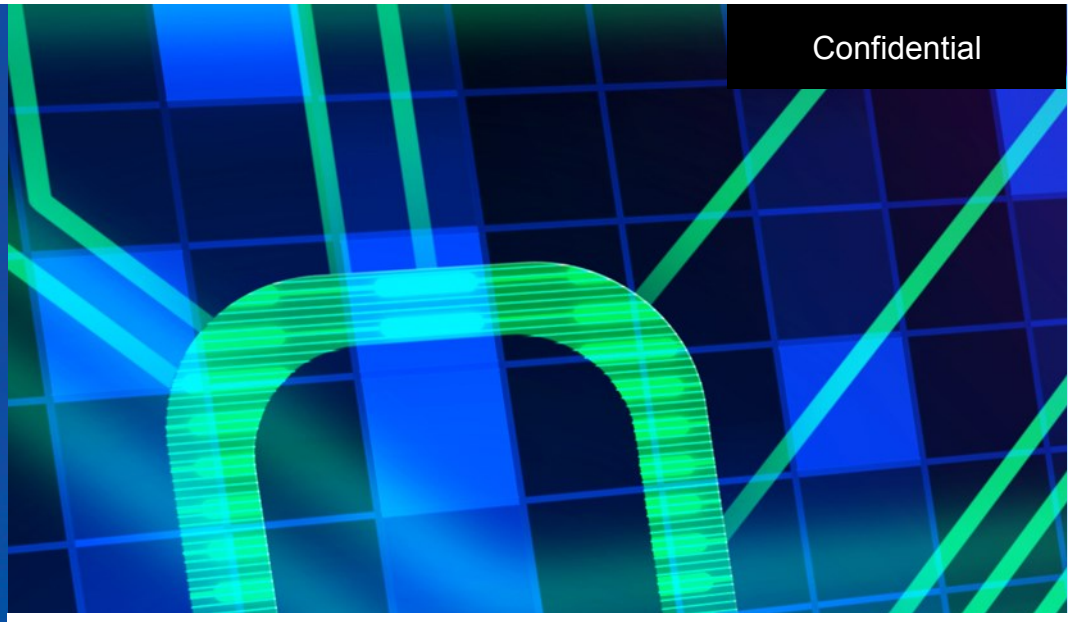
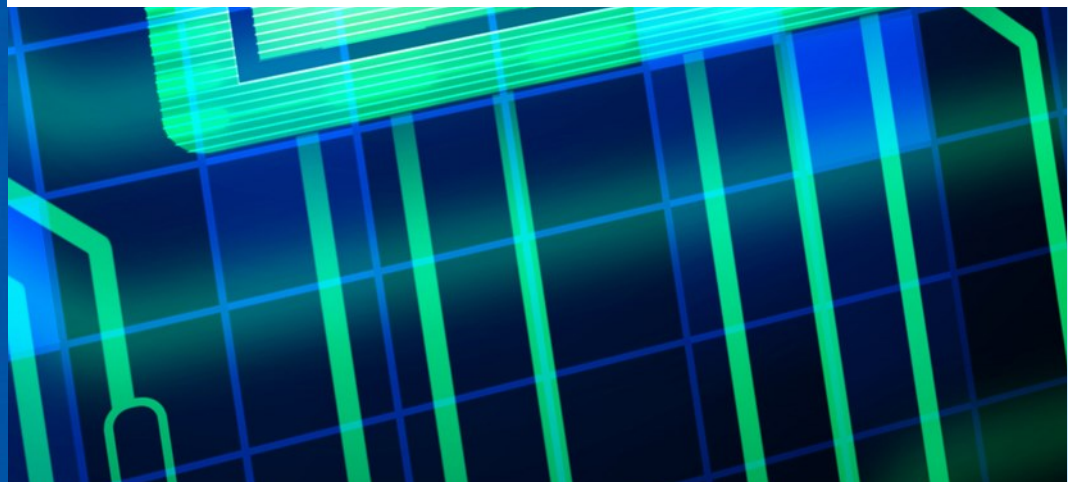
Confidential



PARTICIPANT'S GUIDE

"In A Flash! A Lesson on Cybersecurity"

Updated April 2016



CONTENTS

ISSUES AND RESOURCES FOR PARTICIPANTS

The film is structured in three parts to allow discussion at the end of each part. The topics below are suggestions for DLA Piper presenters to raise as topics for discussion at the end of each portion depending on the time allotted for the presentation. The total running time of the film is approximately 45 minutes.

In addition to raising some of the questions below, presenters should also encourage members of the audience to suggest questions or issues that they identify and consider important. A series of general topics and questions is also provided for additional discussion following the film if time permits. These additional discussion points also can be introduced as themes prior to showing the film.

PART I: DISCUSSION TIME OF APPROXIMATELY 15 MINUTES

Model Rule 1.1

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Model Rule 1.4

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation

Has BaySan Global done adequate "cyber diligence" on its third-party service providers and vendors, including ArdoTech? What are the potential consequences of a company's failure to do so? Should vendor and supply chain risk be a part of BaySan Global's cyber-risk management strategy? What should BaySan Global require of its vendors to mitigate supply chain risk?

- During the audit committee meeting, Gao Boro, the Deputy General Counsel for BaySan Global, makes the case for prioritizing data security and breach response. She notes that BaySan Global is not holding its vendors to the same security standards that the Company itself follows.
- The supply chain is a key area of risk (e.g., HVAC entry point to big retailer networks).
- In some countries, there is a clear obligation on the "data owner" to conduct diligence on its third party service providers. Even absent a specific legal obligation, a company should conduct appropriate diligence (what is appropriate will depend on the type of work being performed by the service provider) on each service provider.
- Contractual requirements should include specific security measures, auditing, breach response responsibilities (including, requiring the service provider to provide notice of suspected breaches, allocation of responsibility in the event of an actual breach).

Model Rule of Professional Conduct 1.3: Diligence

A lawyer shall act with reasonable diligence and promptness in representing a client.

Model Rule of Professional Conduct 1.13(a): Organization as Client

A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.

Should cybersecurity be considered just an IT issue? Should the examination of cybersecurity risks be the responsibility of the Audit Committee, a Risk Committee or the whole Board? Or should the Board create a separate Cyber Committee?

- Max Levine, an audit committee member, admits that he is not "completely on top of these cyber issues" and the Audit Chair says that the Company is in "good hands" with the Chief Information Officer and Chief Information Security Officer.
- Oversight is required and a risk committee, if one exists, is a good place to house the oversight function.

What procedures should the Company put in place to ensure that the Board has adequate access to cybersecurity expertise? Do Boards need one member who understands technology? How else can they acquire technology sophistication? Should Board members be required to participate in relevant education programs? Should the Board schedule briefings from third party experts? Hire advisors to consult with the Board on cybersecurity issues? Allow the Board to pose questions to senior management responsible for addressing cybersecurity threats, such as the CIO and CISO?

- As noted above, the Audit Committee admitted that it lacked expertise in cybersecurity issues.

- It is important for the board to have sufficient expertise to oversee cyber risk management and ensure that adequate resources are devoted to it.
- Audit Committee doesn't protect privilege.

What are the dangers of assuming that hackers are more likely to target someone else? Do cyber attacks always follow a predictable pattern? Why are service providers who hold other companies' data potential targets?

- When asked by the audit committee how the company rates as a potential target for a cyber attack, Darrin Riley, the Chief Information Officer, downplays BaySan Global's risk. According to him, the Company's risk is low to moderate because it doesn't fit the profile of companies that hackers typically target (e.g., it doesn't have "troves of credit card and personal data"). Felicity Allen-Grey, the CISO, disagrees.
- Complacency is a leading cause of data breaches, and it can take many forms. Complacency can mean assuming that because your company is too big or too small or that it doesn't hold substantial amounts of sensitive computer data that it is unlikely to be a victim of a cyber attack. It can also take the form of failing to appropriately vet suppliers or adequately insure against cyber risk.
- Complacency makes it difficult to defend against cyber attacks because it creates vulnerabilities throughout the supply chain.
- Service providers who hold lots of client data can be interesting targets for hackers.
- Given that cyber attacks are a virtually unpredictable risk with far-reaching consequences, no company, large or small, can afford to be complacent.

How important is it for CIOs and CISOs to have a working relationship? Would it be better for BaySan Global if the CISO reported to the Chief Risk Officer or CEO rather than the CIO?

- The CIO and the CISO at BaySan Global don't see eye to eye on many key issues.
- Whether the CISO should report to the CIO, Chief Risk Officer or the CEO has been the subject of intense debate. Some studies have found that organizations where the CISO reports to the CIO experience more downtime related to cyber incidents and higher financial losses.
- See Clint Boulton, "Readers Debate CIO, CISO Reporting Structure," *Wall Street Journal*, Feb. 10, 2015, available at: http://blogs.wsj.com/cio/2015/02/10/readers-debate-cio-ciso-reporting-structure/

Model Rule 5.3

With respect to a non-lawyer employed or retained by or associated with a lawyer:

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Baysan has a sophisticated cybersecurity operation, as the GC Raymond Cate notes. What is wrong with Baysan's assumption that it could create exceptions on security requirements for key suppliers, given that it has a robust cyber security program?

- General Counsel Raymond Cate says that BaySan Global has a great team, protocols, and a response plan, and Borro notes that the company regularly runs penetration tests and tabletop exercises.
- Attackers can enter through any vendor that has direct access to your company's network.
- Malware is often very difficult to detect and vendors – and your own IT Department – may miss it

Since smaller firms are often used by cyber attackers as an entry point into larger organizations, how important is vendor management? In addition to building assurances into the agreement with AndroTech regarding its plan for implementing security upgrades, how else should BaySan Global have addressed the risk of this potential point of vulnerability?

- During the meeting between BaySan Global and ArdroTech to discuss the anticipated award of a major new contract, Felicity Allen-Grey, the CISO, raises concerns about ArdroTech's risk of a data breach.

PART II: DISCUSSION TIME OF APPROXIMATELY 15 MINUTES

What other crisis management strategies could BaySan Global have employed?

- During the global breach response team briefing, Darrin Riley, the CIO, is the only one who appears to believe that giving in to the extortion demand is the wrong strategy.

What are the weaknesses in this approach to managing the crisis? Is giving in to an extortion demand the only, or most effective, way to protect the Company's brand and reputation?

- The General Counsel, Raymond Cate, says that paying off the extortion demand for $50 million dollars will "seem like a bargain" compared to the potential financial and legal fallout.
- Companies that are appropriately prepared to address cyber incidents, including potential blackmail, generally have more options to them in evaluating how to respond to an extortion demand.

- For example, if data are backed up frequently and operations can be switched over to a separate and secure environment, or if the data is no longer necessary (and/or can be easily replicated), companies may not need to give into the blackmail demand.
- In breaches involving extortion demands, companies should seriously consider involving law enforcement.

Model Rule of Professional Conduct Rule 1.2 (d) Scope Of Representation And Allocation Of Authority Between Client And Lawyer:

A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.

What preventative measures could the Company have employed to head off the crisis? What are the important features of an effective crisis management plan?

- During the conference call with the Board to authorize the extortion payment, Board Member Max Levine says that BaySan Global will be just opening the door to more hacks.
  What preventative measures could the Company have employed to head off the crisis?
- A comprehensive disaster recovery program, including appropriate data backups and an appropriate and regularly tested disaster recovery plan and processes, may have helped Company avoid the extortion demand because Company may have been able to switch over to its backup data center.
- Both BaySan Global and ArdoTech hurry to implement crisis management plans.
  What are the important features of an effective crisis management plan?
- Important considerations include whether a company's crisis management or incident response plan has been tested and is therefore ready to be implemented as soon the company learns of a breach.
- Many companies either do not assess the readiness of their incident response teams or fail to do so on a regular basis.
- Incident response teams are important because they don't simply "clean up" security breaches. They also seek the root of the problem and manage and contain fallout from the breach.
- DLA Piper offers clients a model breach incident response plan for clients to adapt to their regulatory obligations and organizational structures.
- See Ponemon Institute, *Cyber Security Incident Response: Are We As Prepared As We Think?*, Jan. 2014, available at: https://www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf.

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized

access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with non-lawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4]. [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

What are the potential consequences of Thomas's failure to report the incident to Wu? Does it matter that the laptop was out of his sight for a short period of time? What are the potential risks associated with not having a clear and documented process for reporting and addressing lost and stolen laptops?

- When the ArdroTech management team gathers to discuss the BaySan Global breach and the revelation that the hackers found a gateway through the ArdroTech system, Garrett Thomas, ArdroTech's Chief Development Officer, has a flashback to his business trip to Mexico City, in which he failed to follow up on his initial attempt to report a missing laptop.
- Lost or stolen laptops offer hackers the means to penetrate corporate networks that would otherwise be difficult to access. Hackers are employing increasingly sophisticated—and creative—methods to gain access to companies' systems. See Nicole Perloth, "Hackers Lurking in Vents and Soda Machines," New York Times, Apr. 7, 2014, available at: http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html?_r=0.

What are some common sense precautions employees can take when traveling overseas? Should employees be required to use a "clean" laptop and smartphone when traveling overseas, particularly in countries with a reputation for engaging in cyberespionage? What are some other precautions employees could take?

- Garrett Thomas misplaces his laptop for what appears to be several hours on a business trip to Mexico City.
- Laptops and portable devices should be clean or should never leave the possession of the employee, particularly in risky countries.
- Mexico is not known as a particularly risky country in this regard.

Should ArdoTech have done a better job of training its employees on the security risks associated with misplaced or stolen laptops and the security protocols that must be followed in the event of misplaced or stolen laptops? What are best practices for security training? How often should employees be trained? What is the best way to help employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources?

- Garrett Thomas fails to report the misplaced laptop to Feng Wu because he is embarrassed that he let it out of his sight.
- Companies should train their employees in appropriate response to a lost or stolen device, whether company-owned or BYOD where such device is used for work purposes. That said, employees don't always follow policies and training instructions.
- The "right" answer to security training is company-specific. Often training at onboarding and annually or bi-annually thereafter is appropriate for most employees. However, certain roles warrant additional and more customized training.

Is she correct that the Company would have a reasonable defense if the information regarding Garrett Thomas's possession of MZ3's trade secrets comes to light? Was her response to the discovery that Thomas stole MZ3's trade secrets appropriate? What protocols should MZ3 have put in place to protect its trade secrets?

- During the security breach update in the ArdroTech CEO's office, CEO Tamara Milken asks whether the company has a formal policy regarding trade secrets.

How did the breakdown in protocol occur? Should the IT worker have reported the fact that he found Carter Rixman logged into a computer when everyone was supposed to be logged out to preserve evidence? What measures could BaySan Global have taken to protect itself from an insider threat?

- The CISO informs the COO that the Company is prohibiting members of the team from gaining physical access to the equipment because, although the Company is operating as if the breach is an outside breach, she can't be sure.
- BaySan disregarded not only vendor but also insider risk. Disgruntled insiders, particularly disgruntled IT personnel, can pose major security risks.

- For the first breach, the company hires LMP Cyber Forensics. For the second breach, outside counsel hires LMP Cyber Forensics.
  What are the benefits of having outside counsel hire the cyber forensics company? What are the benefits of engaging outside counsel and a cyber forensics firm before a breach actually occurs?
- Involving outside counsel at the outset of the investigation improves arguments for privilege protections attaching against later discovery of materials related to a company's internal investigation and remediation efforts.
- It allows the Company to uncover the root cause of the breach while limiting its potential litigation risk.
- Outside counsel can also help the Company navigate the maze of statutory, regulatory, and contractual requirements.
- See Benjamin C. Linden, Richard M. Martinez, and Seth A. Northrop, "Use Outside Counsel to Control Data Breach Loss," *Bloomberg Law*, March 21, 2014, available at: http://www.bna.com/outside-counsel-control-n17179888989/.

Model Rule of Professional Conduct 1.6: Confidentiality of Information

Will the Company be adequately covered through its comprehensive general liability insurance, as the COO suggested to the Audit Committee at the beginning of the movie?

- The COO informs outside counsel that the Company doesn't have cyber insurance.
- Although in the past companies took that approach, today's standard is to purchase standalone cyber insurance policies to cover risk associated with breaches of personal information (although they cannot protect against reputational risk and may not cover foreign government attacks).

PART III: DISCUSSION TIME OF APPROXIMATELY 15 MINUTES

What is the business impact of a data breach? What can companies do to retain clients after a major breach?

- The CEO of BaySan Global's largest client explains that sticking with BaySan Global will, in the short term, give the Company more pricing leverage.
- Data breaches are more than just breaches of security. They are also breaches of trust between a company and its customers.
- After a breach, companies need to focus on taking actions to regain clients' trust and repair the company's reputation.
- This can include providing remediation to customers as warranted and explaining clearly how the incident occurred and what the company has done to prevent a similar incident from occurring in the future.

What are the potential costs associated with breach remediation?

- The breach severely harms BaySan's reputation, including loss of customer confidence and public disclosure of harmful information.
- Breaches of unencrypted sensitive personal information often trigger public data breach notice obligations, as occurred here.
- But they also can trigger contractual notice obligations and violate confidentiality obligations to business customers, and can result in loss of trade secrets and disclosure of sensitive internal communications.
- The average cost in 2014 of a data breach that requires public notification has been measured at $200 per record that was breached, including harm to reputation and loss of good will. That same study, however, found that the cost per record lost went down significantly for companies that were prepared to handle data incidents.

ADDITIONAL DISCUSSION

- What could BaySan Global have done to mitigate the risk of a data breach?
- What measures should it have taken to reduce the cost of breach remediation?
- What were the critical missteps that led to the data breach?
- Should BaySan Global have contacted law enforcement?
- Did BaySan Global's approach to security leave it vulnerable?
- Its complacency?
- Employees' egos and self-dealing?