DLA PIPER

Cybersecurity Legal Issues

("In a Flash" – Lessons in Cybersecurity)

Table of Contents

At the end of each part of the film, we will pause to provide instruction for attorneys about the legal and ethical topics presented in the film. There will be opportunities for discussion, question and answers after each part.

Part I:
Cyber Diligence & Cyber Governance

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.

Ethical Obligations – Cyber Diligence

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

Cyber Diligence

During the audit committee meeting, Gao Boro, the Deputy GC for BaySan Global, made the case for prioritizing data security and breach response. She noted that BaySan Global is not holding its vendors to the same security standards that the Company itself follows.

- BaySan Global should have:
  - conducted adequate "cyber diligence" on third-party service providers and vendors, including ArdoTech. Failure to do so can result in many devastating consequences.
  - taken steps to appropriately address vendor and supply chain management in its cyber-risk management strategy.

NIST CYBERSECURITY FRAMEWORK:
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Cyber Diligence

- 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).

SAMPLE VENDOR CONTRACT PROVISIONS - ALLOCATION OF CYBERSECURITY RISK (DLA PIPER 2015)

Ethical Obligations – Cyber Governance

- **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.

Cyber Governance

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 CIO and CISO.

- Cybersecurity is no longer just an IT issue.
- Companies must determine whether cybersecurity risks should be managed by the Audit Committee, a Risk Committee, the whole Board, or a newly-created Board Sub-Committee
- Oversight is required and a risk committee, if one exists, is a good place to house the oversight function.

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.
- Companies must implement procedures to ensure that the Board has adequate access to cybersecurity experts, who may or may not hold Board seats.
- Companies could consider requiring Board members to participate in relevant education programs.
- The Board should consider: briefings from third party experts and how it can pose questions to senior management responsible for addressing cybersecurity threats, such as the CIO and CISO.
- Audit Committee doesn't protect privilege.

Cyber Governance

When asked by the audit committee how the company rates as a potential target for a cyber attack, the CIO downplayed BaySan Global's risk and suggested 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"). The CISO disagreed.

- Assuming that hackers are more likely to target someone else is a dangerous assumption. Cyber attacks do not always follow a predictable pattern.
- Complacency is a leading cause of data breaches, and it can take many forms. Complacency can mean assuming that because the company is too big or too small or doesn't hold substantial amounts of sensitive computer data, 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.

Cyber Governance

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.
- CIOs and CISOs with a strong working relationship strengthen a company's overall cybersecurity maturity.
- Companies should carefully consider the CISO reporting structure (e.g., to the Chief Risk Officer or CEO vs. the CIO)

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/

Cyber Governance

GC 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.

- BaySan has a sophisticated cybersecurity operation, as the GC Raymond Cate noted. BaySan should not assume, however, that it could create exceptions on security requirements for key suppliers, even though it has a robust cyber security program.
- 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.

- **SAMPLE VENDOR CONTRACT PROVISIONS - ALLOCATION OF CYBERSECURITY RISK** (DLA PIPER 2015)
- **DLA PIPER SAMPLE VENDOR SECURITY DILIGENCE QUESTIONS**
- **DLA PIPER SAMPLE DETAILED VENDOR SECURITY ASSESSMENT QUESTIONS**

Model Rule 5.3

With respect to a nonlawyer 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 nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

Model Rule 5.3 (cont.)

(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.

Part I Conclusions

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

- Attackers can enter through any vendor that has direct access to your company's network.
- Vendor Management is crucial.
- Smaller firms are often used by cyber attackers as an entry point into larger organizations.
- In addition to building assurances into the agreement with AndroTech regarding its plan for implementing security upgrades, BaySan Global should have addressed the risk of this potential point of vulnerability throughout the project lifecycle.

Part II:

Cyber-risk Management, Incident Response and Security Protocols

Cyber-Risk Management

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.

- BaySan Global could have employed other crisis management techniques, including drawing from published industry recommendations.

DEPARTMENT OF HOMELAND SECURITY (DHS) GUIDANCE: CYBER RISK MANAGEMENT PRIMER FOR CEOS

Identifies key concepts to evaluate in implementing a cyber plan.

- http://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf

Cyber-Risk Management

The GC, Raymond Cate, said that paying off the extortion demand for $50 million would “seem like a bargain” compared to the potential financial and legal fallout.

- The company exhibited weaknesses in its approach to managing the crisis. Giving in to an extortion demand is not the only, or most effective, way to protect the Company’s brand and reputation.
- 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.

Ethical obligations

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.

Incident Response Plans

- 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 **DLA PIPER SAMPLE INCIDENT RESPONSE PLAN**

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.

Security Protocols

The Company could have employed protective measures 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.
- An effective crisis management plan is crucial to cyber-resilience.

Security Protocols – Other Resources

WIRE TRANSFER PHISHING – AN OLD SCAM RETURNS: SIMPLE STEPS TO PROTECT YOUR ORGANIZATION

By Tara Swaminatha
DLA Piper Cybersecurity Alert (September 2015)
https://www.dlapiper.com/en/us/insights/publications/2015/08/wire-transfer-phishing-an-oldscam-returns/

FINRA GUIDANCE

FINANCIAL INDUSTRY REGULATORY AUTHORITY (FINRA): REPORT ON CYBERSECURITY PRACTICES, FEB. 2015.

In the Report, FINRA identifies an approach to cybersecurity for entities to consider, recognizing that there is no one-size-fits-all approach to cybersecurity.

https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

FTC Guidance

FEDERAL TRADE COMMISSION (FTC): PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, JUNE 2015

Designed to assist businesses in developing greater security to protect consumers' personal information. Guide based off of the approximately fifty (50) data security cases that the FTC has brought against companies throughout the years.

https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting personalinformation-guide-business_0.pdf

FCC Guidance

FEDERAL COMMUNICATIONS COMMISSION (FCC): CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES (REPORT) BY THE COMMUNICATIONS SECURITY, RELIABILITY AND INTEROPERABILITY COUNCIL (CSRIC) FOR COMMUNICATIONS PROVIDERS

CSRIC is a federal advisory committee with members from the private sector, academia, engineering, consumer/community/non-profit organizations, and government partners (Comment cycle on this report closed at the end of June 2015.)

http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf

Ethical obligations

Model Rules 1.1, 5.1, 5.3

Acting Competently to Preserve Confidentiality

A lawyer must 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.

Ethical obligations

Model Rules 1.1, 5.1, 5.3 (cont.)

Acting Competently to Preserve Confidentiality

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 nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4]. [19]

Model Rules 1.1, 5.1, 5.3 (cont.)

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.

Security Protocols

Thomas's failure to report the incident to Wu resulted in several undesirable consequences. The fact that the laptop was out of his sight for a short period of time does not serve as a mitigating factor.

- Having a clear and documented process for reporting and addressing lost and stolen laptops mitigates this serious risk.
- 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.

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.

Security Protocols

Garrett Thomas misplaced his laptop for what appeared to be several hours on a business trip to Mexico City.

- When travelling overseas, employees can take common sense precautions to reduce risk.
- Companies could consider requiring employees to use a “clean” laptop and smartphone when traveling overseas, particularly in countries with a reputation for engaging in cyberespionage.
- 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.

Security Protocols

ArdoTech could 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.

- 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.

Security Protocols – Other Resources

COURTS' DETERMINATION OF STANDARD OF CARE FOR CYBERSECURITY PRACTICES

- *Cooper v. Eagle River Mem. Hosp., Inc*., 270 F.3d 456, 462 (7th Cir. 2001)
- *Transp. Ins. Co. v. Detroit Edison Co*., No. 239142, 2003 WL 22956418, at *2 (Mich. Ct. App. Dec. 16, 2013) (citing *Zdrojewski v. Murphy*, 254 Mich. App 50, 62–63 (Mich. Ct. App. 2002)).
- *Titchnell v. U.S.*, 681 F.2d 165, 173 (3d Cir. 1982)
- *Darling v. Charleston Cmty. Mem'l Hosp*., 211 N.E.2d 253, 257 (Ill. 1965)

OTHER RESOURCES

- *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 954-955 (S.D. Cal. 2014).
- *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14-2522 (PAM/JJK)
- **NEW U.S. SANCTIONS PROGRAM TO COMBAT CYBERCRIMES: 3 ACTION STEPS FOR TECH COMPANIES**, by Jim Halpert, Lawrence E. Levinson, Richard Newcomb, Rochelle Eva Stern, Tara Swaminatha and Sydney M. White, DLA Piper Cybersecurity Alert (September 2015) https://www.dlapiper.com/en/us/insights/publications/2015/04/new-us-sanctions-program-tocombat-cybercrimes/

Security Protocols

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.

- If the information regarding Garrett Thomas's possession of MZ3's trade secrets comes to light the company's defense may be impacted.
- Companies should have formal policies regarding trade secrets, including specific protocols employed to protect trade secrets.

Security Protocols

A breakdown in protocol occurred - the IT worker could have reported the fact that he found Carter Rixman logged into a computer when everyone was supposed to be logged out to preserve evidence. BaySan Global should have taken stronger methods to protect itself from an insider threat. The CISO informed 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.

- If outside counsel hires the cyber forensics company, its analysis will be privileged and protected by attorney work product doctrine.

Security Protocols

- 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.
- This 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.

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

Companies should ensure adequate coverage through its comprehensive general liability insurance.

The COO suggested to the Audit Committee at the beginning of the movie. The COO informed 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:

Business Impact of Data Breaches

Business Impact of Data Breaches

The CEO of BaySan Global's largest client explained that sticking with BaySan Global would, 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.

Potential costs associated with breach remediation

The breach severely harmed 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 (including reputational harm and loss of good will). The cost per record lost was significantly less for companies that were prepared to handle data incidents.