Cybersecurity Conference Key Takeaways

On November 28, 2017, Cleary Gottlieb, in partnership with K2 Intelligence and BlueVoyant, hosted an afternoon conference in New York on "Cybersecurity Lessons from the Boardroom and C-Suite to the Front Lines," featuring data security experts, law enforcement, regulators, board members, and in-house counsel of global companies.

Below are the key takeaways from the two plenary discussions and three break-out sessions.

Before the Call: Current Best Practices for Boards and Management to Mitigate Cyber-Risk

The first session, moderated by **Katherine Mooney Carroll**, *Partner*, Cleary Gottlieb, featured contributions from:

Admiral Mike Mullen, *Director*, General Motors and Sprint Corporation; *former Chairman*, Joint Chiefs of Staff

Jim Rosenthal, *CEO*, BlueVoyant; *former Chief Operating Officer*, Morgan Stanley

Gerald Werner, *Global Director of Information Security*, K2 Intelligence; *former Chief Information Security Architect*, National Football League

Pamela Marcogliese, *Partner*, Cleary Gottlieb

The session began with a discussion of the appropriate role of the board of directors in overseeing the management and mitigation of a company's cyber-risk. While various laws and regulations set forth certain minimum obligations (for example, recent cybersecurity regulations for entities regulated by the New York Department of Financial Services require the board to receive an annual written report on cybersecurity), the panel noted that complying with such requirements represents the floor of what responsible boards should be doing with respect to cybersecurity.

Admiral Mike Mullen explained that boards should consider treating cybersecurity as a unique type of risk rising to the level of an "existential threat." The panel repeatedly underscored the gravity and pervasiveness of cybersecurity threats, at one point noting, "there are two kinds of companies: companies that believe they've been attacked and companies that don't believe they've been attacked because they haven't yet realized it's already happened."

As a result, a board should, among other things, ensure that the company is hiring experts, allocating sufficient resources, and implementing effective policies to adequately protect the company against material cybersecurity risks. In addition, the panel suggested that boards consider the feasibility of creating a special committee or subcommittee that is dedicated to cybersecurity issues and that can develop the expertise necessary to understand and address such complex matters in light of each company's specific circumstances, available resources, and composition of the board and management. The panel also discussed the benefits of appointing a director with significant technical expertise to the board. For companies where creating a special committee or appointing a director with technical expertise is not feasible, the panel discussed engaging an outside expert to assist with risk assessment, monitoring, and remediation of cyber-concerns.

The panelists also shared their advice for mitigating cyber-risk, including:

- Establish relationships before a breach occurs, including with law enforcement, regulators, outside counsel, forensic firms, and cyber-insurers.
- As part of the incident response plan, have a communications plan for investors, customers, counterparties, and regulators that is as comprehensive as possible and includes the appropriate members of management, legal,public relations, and investor relations.
- Identify the company's "crown jewels" – i.e., its most important assets and sensitive information – and use that information to determine security priorities (including whether it is possible to implement additional security barriers to accessing such information).
- Hire a "red team" to conduct vulnerability and penetration testing on a regular basis, and use the results to create and regularly update an incident response plan.
- Practice the incident response plan, such as through tabletop exercises, in as much detail and as realistically as possible.

The panel also noted that information sharing bodies, such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC), allow the public and private sectors to mutually benefit from pooled data about vulnerabilities, patches, indicators of compromise, and effective defensive measures.

The panel noted that companies should be cautious about purchasing and implementing untested technologies that may claim more than they can deliver or that may prove unproductive in the long term. The panel advised that a certain degree of consolidation in the market for such technologies is likely to occur.

After the Call: Managing the Regulatory and Litigation Fallout from a Breach

The second session, moderated by **Jonathan Kolodner**, *Partner*, Cleary Gottlieb, featured contributions from:

David Shonka, *Acting General Counsel*, Federal Trade Commission

Timothy Howard, *Co-Chief*, Complex Frauds and Cybercrime Unit, United States Attorney's Office, Southern District of New York

Austin Berglas, *Senior Managing Director*, BlueVoyant

Rahul Mukhi, *Counsel*, Cleary Gottlieb

This session focused on steps that a company should take in the aftermath of a cyber-breach. The panel noted that ideally a company will immediately execute its incident response plan, which should include the retention of outside counsel, who are best positioned to oversee the investigation of a potential breach so that communications with the internal response team and other outside experts, such as a forensics team or public relations firm, may be protected by attorney-client privilege.

The panelists sounded a note of caution, however, against assuming that the attorney-client privilege and work product doctrine will protect all communications surrounding a potential cyber-incident, since privilege is intended only to shield communications between lawyers and their clients concerning *legal advice*. Companies should take a nuanced approach and consider clearly establishing and documenting particular communications channels and workstreams for the purpose of obtaining legal advice or in anticipation of litigation.

In instances when forensic firms are hired before counsel, supervision of the forensic firm should be transferred to outside counsel upon their hiring, and the work plan should be updated to reflect that the forensic firm is assisting outside counsel in connection with the provision of legal advice.

The panel also discussed using forensic experts to identify and repair the exploited vulnerability as soon as possible, and then to identify, among other things, any compromised data, the encryption status of any such data, the affected data subjects, the subjects' locations, and the risk of harm posed by the breach to their data. These factors can impact the company's data breach notification obligations, which vary by state, country, and industry. The panel noted that in some cases, notification to regulators and/or data subjects could be required in as few as 72 hours after becoming aware of the breach (and in some jurisdictions, it could be even sooner). The panel also discussed that any public statements about a breach should be carefully vetted and that, for companies with SEC reporting obligations, the SEC's cybersecurity disclosure guidance should be followed. The panel noted that the SEC recently announced that it would be issuing updated cybersecurity guidance.

The panelists then evaluated the benefits of working with law enforcement in the wake of a breach. Timothy Howard of the U.S. Attorney's Office noted that the FBI and other law enforcement agencies can be helpful in fully investigating the incident, as the FBI has access to greater resources and sources of information, particularly internationally. The government's resources allow it to obtain and relay information that would otherwise be impossible for the company to learn, for example, identifying additional accounts compromised or stolen materials stored on offshore servers. In addition, cooperating with law enforcement can serve as a deterrence to cyber-criminals, who may come to view the company as being too much of a risk to hack.

Responding to perceived concerns of companies about the potential invasiveness of law enforcement in the wake of a breach, Austin Berglas of BlueVoyant, a former FBI agent, noted that FBI involvement would not ordinarily impact ongoing operations or result in unnecessary downtime. The panel also observed that civil regulators (such as the FTC) generally respond positively when a company voluntarily cooperates with law enforcement after a breach.

The panel then discussed the variety of litigation risks posed by a cybersecurity incident, including lawsuits brought by the FTC, consumers and employees whose data was compromised, financial institutions paying for losses incurred after a breach, contractual counterparties, shareholders, and state attorney general offices. FTC Acting General Counsel David Shonka explained that the Federal Trade Commission has broad authority to investigate and prosecute unfair or deceptive trade practices, which can include "unfair" cybersecurity practices and "deceptive" data security and privacy claims, without the need to prove actual harm or injury to a consumer. The panel also considered the question of director liability. While no shareholder cases brought after a cyber-breach have resulted in a finding of a breach of fiduciary duty to date, directors should be on notice that they may be exposed to some degree of litigation risk in connection with their oversight of cybersecurity.

Finally, the panel discussed remediation, including curing any identified gaps and vulnerabilities, ranging from misconfigured

infrastructure to unpatched environments to re-training of employees. Companies should also consider conducting vulnerability scans on a quarterly basis and penetration testing on an annual basis, in each case on the entire environment, as hackers often penetrate a network at its weakest point and then lateral over to more critical areas. To that end, the panel suggested focusing on endpoint security protection and noted that the organizations with the most visibility into their networks are often the quickest to recover.

Looking forward, the panel remarked on the proliferation of competing and overlapping laws and regulations and noted that it remained to be seen whether regulators would become more aggressive, particularly with the potential for greater penalties on the horizon (such as with the implementation of the EU General Data Protection Regulation) and whether this leads to a "race to the top" among regulators, particularly in light of public fallout surrounding recent high-profile data breaches.

Tabletop Exercise: Responding Effectively to a Cyber-Incident

This session included a panel featuring contributions from:

Leonard Bailey, *Senior Counsel for National Security*, Computer Crime and Intellectual Property Section, U.S. Department of Justice

Gerald Werner, *Global Director of Information Security*, K2 Intelligence; *former Chief Information Security Architect*, National Football League

Alexis Collins, *Senior Attorney*, Cleary Gottlieb; *former Counsel to the Assistant Attorney General for National Security*, U.S. Department of Justice

Michael Krimminger, *Partner*, Cleary Gottlieb; *former General Counsel*, Federal Deposit Insurance Corporation

Louise Parent, *Of Counsel*, Cleary Gottlieb; *former General Counsel*, American Express

The interactive session focused on the importance of creating detailed workflows and procedures for responding to data security incidents.

First, the panelists introduced a scenario in which a hypothetical New York-based financial services company, ACME, discovers a large, unknown encrypted file on its server. The company's IT support team is certain that the file does not belong on the server. The server, used in conjunction with customer enrollment and customer support services that ACME offers through a third-party service provider, contains customer data. Then, the panelists commenced a discussion with the audience about potential courses of action. Such a discovery raises questions, such as who should be notified of the unknown encrypted file both within and outside of the IT group. The panelists raised the importance of having policies and procedures, codified in an incident response plan, that identify potential triggers for notification to individuals outside of the IT group as well as the individual(s) who should be contacted. Such documentation should also indicate who should investigate the discovery and determine the scope of the investigation.

Next, the audience was provided information that ACME's investigation of the server log files indicated that, for no bona fide reason, the server was communicating with a foreign country. At this stage, the panelists identified parties outside of the IT team who could assist with the investigation, including outside counsel and a forensics team, and noted the potential need to notify the board of directors and even law enforcementat at this point. Some panelists stated that retaining outside counsel at this stage produces a two-fold benefit: outside counsel can provide an additional risk perspective and can help the company more effectively assert attorney-client privilege over certain documents and actions taken under the direction of outside counsel. Relatedly, at this stage, a company may want to consider employing a forensics team to examine the server, encrypted file, and network to determine the cause, nature, and extent of the cyber-incident. A company may be able to successfully claim privilege on certain forensic analysis if the analysis is at the behest and under the supervision of outside counsel.

The panelists also noted that timing is important in investigations of cyber-attacks, particularly if the company is subject to breach notification requirements or supervision by government regulators. Companies should consider that choosing to use a forensics team or outside counsel does not extend the time that a company has to report a breach. It can help companies make appropriate, timely, and accurate reports to applicable authorities to have, as part of the incident response plan, pre-written notification lists and breach notification statements, and clear policies and procedures for when to notify the board of directors, law enforcement, and regulators. Notifying supervisory authorities early may also help reduce legal, financial, and reputational risks, but companies should have an understanding of the cyber-incident prior to reporting. For the purposes of better understanding the incident, a panelist explained that it could be helpful to notify the FBI early on in the investigation, as the FBI may be familiar with the tactics of various actors and may be able to help identify the areas where the company's network may have been compromised.

Finally, the audience was informed that ACME received an email that stated that ACME must pay a hacker 100 bitcoins or else the hacker would announce the breach and sell all of ACME's customer data to the highest bidder on the dark web. The panelists discussed issues surrounding the authenticity of the email, working with law enforcement to learn how similar events have unfolded, and the potential legal implications of paying the ransom, and noted that paying a ransom does not obviate a company from applicable breach notification requirements.

The International Landscape: Complying with the EU's GDPR and Other Data Protection Regimes Outside of the United States

This session included a panel featuring contributions from:

Alfredo Della Monica, *Vice President & Senior Counsel, U.S. Privacy, EMEA Data Protection & Cybersecurity Oversight,* American Express

Samm Sacks, *Senior Fellow*, Technology Policy Program, CSIS

Amélie Champsaur, *Partner*, Cleary Gottlieb

Emmanuel Ronco, *Counsel*, Cleary Gottlieb

The session began with a discussion of the international landscape for cybersecurity and privacy – in particular, how the General Data Protection Regulation (GDPR) is looming large for companies with EU operations, including those with an establishment in the EU, that offer goods and services to EU citizens or monitor EU citizens. The GDPR builds on the current regime with key enhancements such as expanded territorial and extraterritorial reach and enhanced rights for data subjects (including the right to be forgotten or the right to data portability). The overarching message was that if a company processes personal data of EU residents, it has to comply with the GDPR.

The panel also offered insights as to the incentives created under the GDPR – for example, designing systems with privacy in mind, requirements such as regular testing and assessments, reporting breaches, and steep sanctions for violations.

A comparison was drawn between GDPR and the new regulations in China. In China, the law covers cybersecurity and privacy in ways that are much broader than GDPR. One major difference is that under China's law, consent may not be sufficient to allow data to cross borders. Although implementation is still being debated, the panelists indicated it would be practical to assume that certain data will have to be stored locally given the new regulations.

A major theme of the discussion was how to deal with conflicting frameworks and rules, and how to comply with legislation in various jurisdictions – e.g., those that apply to moving data across borders.

Key takeaways included:

— EU legislation (both the existing regime and the future one under the GDPR) involves a very different framework from laws in the United States. U.S. privacy laws tend to be prescriptive and regulated by industry, whereas the GDPR is overarching in design and is industry agnostic. However, China is the broadest in its approach.

— The GDPR has an extraterritorial effect, seeking to apply to companies that are established in the EU or that are established outside of the EU but do business with or monitor individuals in the EU.

— Preparation is key to mitigating risks.

Practical recommendations included:

— Make a self-assessment – map your data, determine which laws apply, and conduct a gap analysis to assess what measures to take and by what deadline.

— If the GDPR applies to some of your processing, use the GDPR requirements as the high-water mark on which to base a core set of principles – however, make them easily amendable with riders on a jurisdictional basis to accommodate local requirements.

— Have a responsible person in charge of managing your compliance program. This person may be a Data Protection Officer, which is a regulated position under the GDPR, or else may be a Chief Privacy Officer.

— When planning your approach and implementing your compliance program, involve critical stakeholders within the system (HR, legal and compliance, IT, procurement).

— Have a law firm with global reach to help communicate between regulators, manage relationships, and find pragmatic solutions to complicated situations.

— If full implementation is not possible, companies at least should create a risk mitigation strategy.

Outlook:

— A scenario similar to the Equifax data breach would implicate several GDPR provisions, such as the principles of "privacy by design" and "data minimization" and the security requirements (which impact both the technology and the personnel). The GDPR would also have required a much faster disclosure to both the regulators and the data subjects and would have exposed the responsible party to large administrative fines (up to 4 percent of the global

turnover of the group for the preceding fiscal year), private damages actions, and criminal sanctions.

— In a cross-border litigation and investigation context, one should look at recent financial regulations and judicial decisions to adopt the best disclosure strategy in light of the data privacy rules (e.g., bank secrecy, blocking statutes, labor law, etc.) and other obstacles, for instance, when mutual legal assistance treaties may be used.

— There is an enforcement paradox: the GDPR has an extraterritorial reach, but when groups do not have a legal entity or branch in the EU, how will enforcement actually take place?

— Although the debate over how to apply the GDPR while recognizing sovereignty of localities is ongoing, there will be a pragmatic approach (according to regulators), but for now preparation is key.

— The trend toward "data sovereignty" and "data localization" in certain countries (e.g., China or Russia) may be explained by the fact that States attempt to not only protect but also control the exploitation of data relating to and produced by their citizens/residents, as personal data is viewed more and more as a type of "natural resource."

— While there have historically been different cultural approaches to privacy in the United States compared to Europe, it is increasingly looking like the U.S. is coming around to the EU model for privacy as U.S. companies are preparing to comply with the GDPR and the EU has adopted a U.S.-style data breach reporting system.

— There are no "one size fits all" solutions – the best strategy is to develop a risk-based approach.

Protecting Yourself in M&A and Vendor Relationships: Evolving Best Practices in Contracts and Diligence

This session included a panel featuring contributions from:

Jordan Arnold, *Senior Managing Director*, K2 Intelligence

Daniel Ilan, *Partner*, Cleary Gottlieb

Jim Langston, *Partner*, Cleary Gottlieb

This session focused on the drastic impact privacy and cybersecurity considerations have had on the M&A landscape and the best practices practitioners should use in identifying, managing, and mitigating related risks.

While a few years ago purchasers rarely conducted any privacy or cybersecurity diligence, and purchase agreements and their ancillary documents narrowly, if at all, reflected the risks related thereto, today substantive diligence in these areas is often imperative and transaction agreements contain robust provisions (sometimes stand-alone data agreements) relating to these risks.

The panelists stressed the importance of considering during diligence both the target's compliance with applicable laws, including privacy, cybersecurity, and data protection laws, and the target's cybersecurity exposure and vulnerabilities.

To conduct a legal review of the target's compliance with applicable laws, purchasers must first identify all applicable laws, which necessitates looking beyond the jurisdictions in which the target and its subsidiaries are incorporated to where the target operates, collects data, processes personal information, and monitors individuals.

The panelists noted that once the applicable laws are pinpointed, a purchaser must determine the appropriate scope of review. To do so, the panelists suggested conducting a risk assessment that includes data mapping and an analysis of the sophistication of the party, its policies, procedures, and controls and adherence thereto. Such assessment will help inform the scope of the diligence that needs to be conducted and assist purchasers in prioritizing.

Based on the assessment, a purchaser may decide to:

- conduct a legal review of the information provided by the target, including its programs, policies, procedures, controls, communications, filings, audits, and assessments and compliance thereto;
- ask the target questions (although, Mr. Arnold warned, the answers are only as good as those responding);
- conduct independent examinations through vulnerability assessments, penetration tests, and audits; and/or
- execute non-invasive investigations through dark web and network activity research.

The panelists emphasized that some diligence, such as examining forums on the dark web, can be done without engaging the target, which may be preferable, particularly in a competitive auction process.

The panelists also highlighted the significant risks of providing data to or receiving software or equipment from a third-party vendor. In particular, Mr. Arnold acknowledged that "the know-your-vendor era is here." To protect itself, a company should properly and continually perform diligence on such vendors as if they were the target in an M&A transaction and push for contractual protections, including indemnities, in its third-party agreements.

The panelists noted that this diligence should inform the purchaser's markup of the purchase agreement and its ancillary documents. Uncovered issues and vulnerabilities can be corrected through interim operating covenants mandating corrective actions.

More generally, privacy and cybersecurity risks can be mitigated by representations (which can also be used to induce disclosure of critical information) and indemnities, coupled with the right to elect not to consummate the transaction, depending on the severity and timing of the breach. In extreme cases, a cybersecurity incident occurring prior to the closing can also lead to a reduction in the purchase price.

The panelists ended by cautioning both sellers and purchasers to seek counsel to ensure compliance with all applicable laws, contractual restrictions, and privacy policies in disclosing any personal data between signing and closing. Even post-closing, the panelists warned, the purchaser will need to carefully consider what steps must be taken to guarantee that its use of acquired data complies with all applicable laws as well as the internal policies and promises of both the target and the purchaser.

Contacts

U.S. and Europe

Katherine Carroll
Partner
Washington, D.C.
+1 202 974 1584
kcaroll@cgsh.com

Amélie Champsaur
Partner
Paris
+331 4074 68 00
achampsaur@cgsh.com

Alexis Collins
Senior Attorney
Washington, D.C.
+1 202 974 1519
alcollins@cgsh.com

Daniel Ilan
Partner
New York
+1 212 225 2415
dilan@cgsh.com

Jon Kolodner
Partner
New York
+1 212 225 2690
jkolodner@cgsh.com

Mike Krimminger
Partner
Washington, DC
+1 202 974 1720
mkrimminger@cgsh.com

Pam Marcogliese
Partner
New York
+1 212 225 2556
pmarcogliese@cgsh.com

Rahul Mukhi
Counsel
New York
+1 212 225 2912
rmukhi@cgsh.com

Louise Parent
Of Counsel
New York
+1 212 225 2232
lparent@cgsh.com

Emmanuel Ronco
Counsel
Paris
+331 4074 68 00
eronco@cgsh.com