DLA PIPER GLOBAL WOMEN'S LEADERSHIP SUMMIT

OCTOBER 16-17, 2018 • THE RITZ-CARLTON CHICAGO

CLE CREDIT OPPORTUNITY

Cybersecurity: Opportunities and Risks with New Technology

October 17, 2018
3:45 p.m. – 5:00 p.m.

DLA PIPER

Speakers

- **Denise Jackson**, Chief Legal Officer, Corporate Secretary
  AMN Healthcare Services
- **Caroline Krass**, Senior Vice President and General Counsel, General Insurance, Deputy General Counsel, *AIG*
- **Rena Mears, Principal**, Data Protection Security, Intellectual Property & Technology Group, *DLA Piper*
- **Rena Hozore Reiss**, Executive Vice President, General Counsel
  Marriott International

Facilitator

- **Stefanie Fogel**, Partner
  DLA Piper

Panel coordinator

- **Maia Sevilla-Sharon**
  Associate, *DLA Piper*

Agenda

- New technology and greater risk of cybercrime
- Principal challenges
- Role of law enforcement
- Best practices
- Risk to Officers and Directors
- Key trends in 2018 and beyond

Overview

The development of technology has improved the efficiency and speed with which global companies conduct day-to-day business in every industry. Technology has impacted core methodology, key analytics, safety, quality and communications. New technology also creates additional vulnerabilities for exploitation of highly confidential data and critical operations.

As the cyber-risk profile evolves, regulators are focused on creating and enforcing data security requirements throughout the company, including at the executive levels. Panelists will explore the role of the general counsel as a strategist in helping the business assess the value and significance of technology with risk mitigation in mind.

Panelists will address best practices for being prepared for a cyberattack, and the role of the legal department in a cross-disciplinary response team. In addition, panelists will focus on increased risks for officers and directors and duties associated with reporting to the executive team and the board.

Q&A – Question 1

- **Question 1:**
  Has new technology created greater risk of cybercrime, and if so, how?
- **Answer:**
  Yes. There is an inevitable tension and conflict between the push for modernization, the growing sophistication in technology, and the resulting increase in data aggregation on the one hand, and cybersecurity on the other hand. The proliferation of social platforms provide new tools to allow cyber criminals to gain access. The scope and amount of available data, including personal data, accessible to cybercriminals is unprecedented. This trend has manifested in terms of impact on privacy.

Q&A – Question 2

- **Question 2:**
  What are some of the principal challenges you face in light of this increased access and exposure?
- **Answer:**
  Data is globalized. Many of us tend to think of information on the national level, but we are all interconnected on a global level. The result of that is diffusion of accountability, which is a significant challenge. Diffusion of accountability manifests in various ways, including by (1) **product manufacturers** – any given product – cars, phones, houses – are made up of components, each of which creates a host of liabilities, but lines of responsibility are rarely if ever drawn; (2) **nation states** – questions of accountability are discussed at the policy level, but does not necessarily translate into action on the ground; (3) **companies** – it is not always clear who at the company is responsible for planning and responding to cyber threats and attacks.

Q&A – Question 2 (cont.)

- The question companies are facing is not whether they have been hacked, but whether they know they have been hacked. Some of the key challenges are complacency, lack of appreciation of risk, and unawareness of the sophistication of cyber criminals, and that complacency exists at all levels of management.

- The supply chain is complex and company leaders often do not fully assess the level of risk within their organization, let alone risks they pose to third parties. Companies must look at concentration of risks outside their immediate circle, they need to perceive themselves as an ecosystem, and that has not really happened yet. When companies look at contractual obligations with various third parties, they are often surprised to see what they have agreed to unwittingly. Contracts frequently impose data security obligations, and then there are bodies of law to be complied with, including the recently-passed General Data Protection Regulation (GDPR).

- Another challenge is resource constraints. There is a tendency to resist spending resources until there is a major attack and impact on the business. Getting business leaders to heed the advice “an ounce of prevention is worth a pound of cure” is always challenging but also very necessary.

Q&A – Question 3

- **Question 3:**
  What is the role of law enforcement in addressing cyber-risks and attacks?
- **Answer:**
  Cybercrime and cyberthreats place many demands on law enforcement agencies, ranging from investigating cyber incidents to securing their own information systems. With growing threats comes the increased presence of law enforcement, which can create challenges for company leadership.

  Some companies find themselves in a position of having to cede or relinquish control of an investigation to government authorities. That creates a host of issues for company leadership, in terms of balancing their own responsibilities with the need to defer to government agencies and facilitate their investigations.

  Another persistent challenge is whether to view law enforcement as a friend or foe, especially when every action or omission is being scrutinized and can subject the company and its officers to liability. Federal agencies appear to be making an effort to partner with companies to foster trust and promote information sharing. With the growing threat of nation states and increased sophistication of these threats, partnering with law enforcement has become critical in defending both corporations and national security. Legal counsel should support that partnership, which can benefit the organization in the long run.

Q&A – Question 4

- **Question 4:**
  What best practices have you employed in your own companies to try to tackle these emerging and growing challenges?
- **Answer:**
  Prioritization - Given limitation constraints, prioritizing resources on high end risks.
  Training – Training must be focused on raising awareness regarding cybersecurity risk and proper messaging (tone at the top) at the highest levels of the company, including the board.

Q&A – Question 4 (cont.)

- **Crisis Management** - An important aspect of training is having a plan in place to respond to an attack, assigning responsibilities, and deciding who has the final word on decisionmaking in a crisis situation. Managing a crisis from a PR perspective is also key, and leaders must be trained about what is appropriate to say and what is not. There are too many examples that we have all seen about business leaders trying to be helpful in diffusing a crisis and ending up sounding tone deaf. So handling crises thoughtfully and responsibly is key.
- **Insurance coverage** – There are more options available to companies now than in the past, and most companies are seeking out cyber insurance protection. Insurance is increasingly getting the "scalpel rather than sledge hammer," so you can find products that address risk a little better than in the past, where it was all or nothing.
- **Competing Interests** – Companies must consider, weigh and balance the following, some of which are in contention with each other (1) privacy of consumer data, a major priority for regulators; (2) protection of assets, the priority for the business; and (3) inconsistent regulations across industries and across jurisdictions.

Q&A – Question 4 (cont.)

- **Preserving the legal privilege** – Response and preparation must be measured and thoughtful – audits create road maps that can be discoverable. That is where the role of in-house counsel is particularly critical, as we are the ones who are expected to make sure the work we are doing is protected by the attorney-client and work product privilege. So there is a tension between making sure that there is awareness on important topics while controlling the flow of information to prevent waiver of the privilege. Be thoughtful about what you put into writing and how broadly you distribute information.
- **Analyze controls** – Companies must continually assess the adequacy of the internal controls they have in place to mitigate cyber risk. It may be worthwhile to have each department run separate analyses and audits because one size does not fit all, and the risks HR is facing may be very different than the risks faced by marketing or other departments. It is advisable not to relegate compliance to one department, but to have various people embedded in different departments to be accountable on this subject.

Q&A – Question 5

- **Question 5:**
  Who are your natural allies in the company, and who are your naysayers that you have to convince? What are the strategies you use to deal with them?
- **Answer:**
  Rena Reiss: Chief Audit Executive, the CFO holding purse strings, the IT team – figuring out your internal network and influencing people is important. If your CEO is not supportive that is an issue, but that is not the end of the discussion. You need a team.

  Topic of legal privilege in the context of globalization will be important here, along with grounds for litigation. The inability to practice within a silo makes it difficult. Sometimes the hardest issue is the politics of cross-jurisdiction, especially if it is a non-US business headquarters. There is not the same level of sharing, and it is hard for people to protect the company. It has become more and more challenging.

Q&A – Question 6

- **Question 6:**
  Based on your experience, are there greater risks of liability for officers and directors? How are those risks mitigated?
- **Answer:**
  Yes, but the scope and nature of the risk is still unclear and evolving. There has not yet been a lawsuit against an officer or director resulting from a cybersecurity incident, but in light of the massive data breaches we have seen and continue to see, courts are going to be inclined to find standing and to hold boards and individuals accountable. So we can expect these issues to arise down the road and need to prepare to defend those kinds of arguments, including arguments about the scope of fiduciary duties and responsibilities and the extent of personal liability.

Q&A – Question 6 (cont.)

- The question arises, does the board need a resident expert? While the CSO is often charged with the responsibility of educating the board, some feel that it is not enough and that individuals with specific cybersecurity and technology expertise should reside within the board.
- Audit Committee members often do not want sole responsibility, so that can be an interesting lead on the board. People don't always appreciate this is not just financial risk, so lines of responsibility are vague. AC is sometimes the front line, but they need to be reporting robustly to the board, and make sure that the whole board is hearing from the IT function, so that it is not being filtered and the board has a chance to ask questions.
- The need for resident expertise will depend on whether CISO is effective in conveying and translating information.

Q&A – Question 6 (cont.)

- When we talk about enterprise risk – even though it may be housed in terms of particular responsibility, the Audit Committee has gotten more comfortable addressing these issues. It is directly tied to comfort with CISO and effectiveness of communication from CISO. From a reporting perspective, CISO gives quarterly presentations to the audit committee, and then they convey to the board. CISO will also give a complete technology presentation. The AC is getting a more in-depth look than board.
- Officers and directors should be taking cyber and privacy very seriously. There is no hiding behind risk. Cyber and privacy have made their way into the top right quadrant of priority. When you present a budget to the board, it is important to get their buy-in about resource allocation and really make the case for why this is a critical investment that can prevent major irreversible problems down the road.

Q&A – Question 7

- **Question 7:**
  What are some of the key trends you are observing in the cybersecurity space, and which concern you the most?
- **Answer:**
  Increased regulation and enforcement – governments are becoming more attuned to cyber risk and less tolerant of what they perceive as corporate negligence.
  - **GDPR** is a good example. GDPR is a very robust regulation and impacts any organization that markets to or retains information from residents of the European Union. Violations of the GDPR can trigger fines of $20 million, so there is not much room for error. Expect regulators to make high profile examples early on.

Q&A – Question 7 (cont.)

- **New York Department of Financial Services' cybersecurity regulation, NYCRR 500**. NYDFS requires that organizations licensed in New York develop, maintain, and monitor a holistic cybersecurity program that is overseen by the senior leadership and officers of the company. The standards outlined in the regulation are the minimum processes, procedures and controls that are needed to protect against data loss. Companies had to file for certification by February, and by September, they were required to implement cybersecurity awareness training and encrypt non-public consumer information at rest and in transit in addition to other practices.
- **New China cybersecurity law** – the reason for the regulation has much less to do with individual rights than with national security.

Q&A – Question 7 (cont.)

- **Increased ransomware attacks** – Keeping patching and updating systems and staying on top of the latest technology is key and will continue to be critical. IoT-based ransomware attacks will likely focus on stealing data or disabling the functionality of a target device. Another possibility is hackers use IoT devices like webcams to funnel traffic to a malware-infected web address.
- **Increased spending on cybersecurity** – As cybercriminals become more sophisticated, companies have no choice but to make this a priority, which translates into increased spending. Firms tracking cybersecurity spending trends have noted a steady increase in spending over the past several years, from approximately $27 billion in 2014 to about $66 billion in 2018. That trend is expected to continue. The average cost of a data breach in 2017 was estimated at $3.62 million, with larger breaches having the capacity to threaten the company's survival.

Q&A – Question 7 (cont.)

- **Increased attacks by nation state actors** – Hacking originating from North Korea, China, and other nation states will continue and intensify.
- **Biometric authentication (and litigation) on the rise** – Biometric authentication is becoming more commonplace in everyday technology devices, including mobile phones and tablets. Fingerprints, face recognition and voice recognition techniques will continue to proliferate, as will litigation over these techniques and privacy concerns associated with them.
- **Increased focus on third-party vulnerability** – Recent examples of breaches have occurred due to vulnerabilities in the supply chain. Increased sensitivity to risk associated with third-party relationships and contracts will continue. Companies must adjust by thinking of themselves as part of an ecosystem.

Denise Jackson
Chief Legal Officer and Corporate Secretary
AMN Healthcare Services

Denise Jackson joined AMN Healthcare in October 2000. Ms. Jackson is responsible for the company's legal, corporate governance, compliance, equity compensation strategies, risk management, real estate, and government and community affairs functions.

From 1995 to September 2000, Ms. Jackson worked for The Mills Corporation serving as Vice President and Senior Counsel from 1998 to 2000. She holds a J.D. from the University of Arizona, a Master of Public Health from The George Washington University, and a Bachelor of Science in Liberal Studies from the University of Arizona.

Ms. Jackson is licensed as an attorney in California, the District of Columbia, Arizona, and New York. Ms. Jackson serves on the Boards of Tractor Supply Company and the Corporate Directors Forum. She previously served on the Board of PipelineRX, LLC where she also held the role of Chairperson of the Compensation Committee and the Board of Girls on the Run International, where she served as Chairperson.

Caroline Krass
Senior Vice President and General Counsel, General Insurance
Deputy General Counsel
AIG

Caroline Krass is Senior Vice President and General Counsel, General Insurance and Deputy General Counsel of AIG. Prior to assuming that role in April 2018, Ms. Krass was a partner in the Washington, DC, office of Gibson, Dunn & Crutcher. As Chair of the National Security Practice Group at Gibson Dunn, Ms. Krass advised clients on the most complicated and sensitive matters involving national security, intelligence, cybersecurity, data privacy, surveillance, economic sanctions, the Committee on Foreign Investment in the United States (CFIUS), government investigations, and regulatory issues. Ms. Krass served as a senior national security lawyer in the Obama and George W. Bush Administrations and is widely known for her experience, both in the US and abroad.

Before joining Gibson Dunn in May 2017, Ms. Krass was appointed to be the General Counsel of the CIA by President Obama, following overwhelming Senate confirmation on a bipartisan basis in March 2014. As General Counsel, she served as the agency's Chief Legal Officer, principal legal advisor to the CIA Director, and a trusted member of the Senior Leadership Team, overseeing more than 150 attorneys and advising on complex, highly sensitive legal and policy issues, including cybersecurity and privacy, foreign investment in the US and export controls, government investigations and litigation, crisis management and congressional relations. From 2011 to 2014, Ms. Krass served as Acting Assistant Attorney General, and before that, Principal Deputy Assistant Attorney General, in the Office of Legal Counsel (OLC) at the Department of Justice, providing legal advice to the Attorney General, the White House Counsel, the National Security Council Legal Adviser, and senior officials at other executive branch agencies on a wide range of complex and significant constitutional, statutory, and regulatory questions.

Ms. Krass served as Special Assistant to the President for National Security Affairs in the Office of White House Counsel from 2009 to 2010. During this time, she dually served as the Deputy Legal Adviser to the National Security Council. From 2007 to 2009, she served as a prosecutor in the US Attorney's Office for the District of Columbia in the National Security Section. Before that, she served as Special Assistant to the Department of the Treasury's General Counsel, as an Attorney-Advisor at the State Department, and as Senior Counsel and an Attorney-Advisor in OLC.

Ms. Krass currently serves as a member of the American Bar Association's Standing Committee on Law and National Security, as a member of the Advisory Board of the Georgetown Law Cybersecurity Law Institute, and as an advisor to two elements of the US Intelligence Community.

Ms. Krass has been awarded numerous honors for her exceptional contributions to national security while in government. She graduated Phi Beta Kappa from Stanford University with a B.A. in International Relations, and she received her J.D. from Yale Law School.

Rena Mears
Principal, Data Protection Security Intellectual Property and Technology Group
DLA Piper

Rena Mears has more than 25 years of experience advising global companies in financial services, hospitality, technology, pharma, biotechnology and consumer products on data risk, privacy, cybersecurity and information security matters. She has built and led teams with the diverse skill sets necessary to manage information assets in the evolving global market. Ms. Mears has worked closely with boards and senior management to evaluate data risk and deploy effective risk mitigation strategies in the enterprise. She has also helped organizations design and implement the effective operational programs, processes and controls required to comply with the legal, regulatory and contractual requirements affecting companies operating in complex regulatory environments.

Before joining DLA Piper, Ms. Mears was the national and global leader of Deloitte's Privacy and Data Protection services, and more recently was managing director at a leading US law firm.

Ms. Mears works closely with lawyers in DLA Piper's global Data Protection, Privacy and Security group – highly rated by Chambers and Legal 500 – to augment the firm's offerings in privacy and cybersecurity assessments, program and control design, data mapping, and program and vendor-risk management.

She has significant experience leading major enterprise initiatives for global companies focused on:

- Data asset risk management services
- Privacy and security program development
- Third-party risk management
- Cybersecurity, data protection, and data breach response
- Forensics, data analytics, and data leakage
- Legal and regulatory compliance
- Privacy and security gap assessments and reporting
- Cross-border data flow compliance and management
- Security and privacy by design in products and services

Ms. Mears' engagements typically involve risk and threat analysis, strategy and program development (including governance, operations, assessment, and reporting), data mapping, controls assessment, and remediation and program sustainment activities. In addition, Ms. Mears has led multi-year engagements dealing with cyberthreats, incident response, and APT analysis for global companies.

She further advises clients on issues involving:

- General Data Protection Regulation; Safe Harbor/Privacy Shield
- US breach notification laws
- Gramm-Leach-Bliley Act
- State privacy and data protection laws
- Health Insurance Portability and Accountability (HIPAA)

She holds the following/certifications: CISSP, CIPP, CISA, CITP. She also is a CPA in Alabama.

Rena Mears received her M.B.A. from Auburn University and her B.A. from the University of Albuquerque.

Rena Hozore Reiss
Executive Vice President and General Counsel
Marriott International

Rena Hozore Reiss is Executive Vice President and General Counsel of Marriott International, Inc. Based in Bethesda, Maryland, Ms. Reiss is a member of Marriott's executive team and leads a global legal team with offices worldwide supporting all facets of Marriott's business, ranging from lodging development and operations to brand, marketing, sales and consumer services, information technology, dispute resolution, intellectual property, compliance and governance.

Ms. Reiss most recently served as Executive Vice President, General Counsel and Secretary for Hyatt Hotels Corporation, headquartered in Chicago, Illinois, overseeing the Hyatt legal department and Hyatt's risk management and corporate transactions teams. At Hyatt, she served as the executive sponsor of the Women@Hyatt business resource group, as well as a Director and Officer of Hyatt Hotels Foundation and Xenia Assurance Company, Inc., Hyatt's captive insurance company.

Prior to joining Hyatt, Ms. Reiss was a Senior Vice President and Associate General Counsel at Marriott, a partner at Counts & Kanne, Chartered, in Washington, DC, and served as an Associate General Counsel for the Miami Herald Publishing Company.

Ms. Reiss sits on the Georgetown University Hospitality Law Advisory Board and is a member of GC50 and the Princeton University Alumni Schools Committee. *Corporate Counsel* awarded Ms. Reiss its Transformative Leadership Award in 2017, and she has been recognized by the ADL Midwest Division as a Woman of Achievement and by the Harvard Law Society of Illinois. She has been profiled in *The Practical Law Journal, The National Law Journal, Diversity and the Bar,* the *Chicago Law Bulletin,* and *Diversity Journal.*

Ms. Reiss is admitted to the bar in Florida and the District of Columbia. She received her A.B. from Princeton University and her J.D. from Harvard Law School. She and her husband Steve, a journalist, have two adult children.

www.dlapiperwomenssummit.com

Stefanie Fogel
Summit Co-Chair
Global and US Co-Chair Leadership Alliance for Women
Co-Chair, Food and Beverage Sector
Partner, Litigation
DLA Piper

Stefanie J. Fogel is Co-Chair of DLA Piper's Food and Beverage sector, focusing her practice on multi-national food and consumer product regulation and compliance, food and consumer product recall response, corporate compliance, and commercial, class action and multi-plaintiff litigation. She represents national and international manufacturers of foods and dietary supplements, retail clothing, manufacturing equipment, chemical products, bio-technology detection devices and a variety of consumer products. Ms. Fogel serves as a national and international advisor to these clients in the area of product safety, cross-border distribution and enforcement, crisis management response, and industry trends. She has extensive experience advising on FDA, USDA, TTB, and CPSC related regulations, including label compliance, claims risk assessment, import and export issues, FSMA, and supply chain management. She is also a seasoned trial lawyer and has represented clients both locally and as national coordinating counsel in toxic torts, consumer fraud, mislabeling and misuse and product liability matters, against individual, multi-district, and class action claims. She has also developed a global multidisciplinary crisis management team to quickly and effectively address issues arising out of recalls, contamination, natural disasters, equipment failure, and environmental leaks and spills.

Ms. Fogel has lectured across the country on subjects relating to food regulatory, litigation and compliance matters, supply chain risk and management, food safety, information management, and in-house and expert witness preparation, as well as civil practice litigation issues. She is well-versed in food and dietary supplement industry trends and has experience necessary to navigate the complex and nuanced food regulatory arena.

Ms. Fogel also concentrates on data strategy, data privacy, and data security process management, records and information management (RIM), and data privacy. She has developed protocols for the implementation of national and international document retention schedules, records management programs, e-discovery strategic plans, and ISO auditing for a variety of industries. She also works with global companies in a variety of industries to develop data strategies integral to new product development.

She is a member of DLA Piper's governing Policy Committee and the Hiring Committee and is also proud to be the co-founder and co-chair for DLA Piper's National Leadership Alliance for Women (LAW) Program.

Ms. Fogel is admitted to practice in Massachusetts, Pennsylvania, and New York and has been admitted in various other states pro hac vice.

Stefanie Fogel received her J.D. from the University of Pennsylvania Law School, and her B.S., *magna cum laude*, from the University of Pennsylvania Wharton School of Finance.