Thursday, Nov. 7, 2019
1:15 PM – 2:30 PM

International Law Symposium – Panel 1 |
The Cybersecurity Alarm Is Blaring—What Are GCs Doing and What You Can Do to Answer the Call

Numerous investors and analysts responding to PwC's recent Global Investor Survey ranked cyber threats as the No. 1 threat to business. Companies are responding accordingly, with nearly all Fortune 500 companies expected to have a Chief Information Security Officer before the end of 2021.

The role of the General Counsel has correspondingly evolved as international players constitute a significant and dangerous feature in the cybersecurity landscape. State actors may use massively funded means to advance their national interests by hacking into U.S. companies' systems—including their IoT products and controls—as well as stealing valuable technology, and customer and supplier data. Terrorist organizations and international criminals may hold hostage, disrupt, and damage government or private enterprise infrastructure. In this increasingly sophisticated area, private denizens who may be outside U.S. jurisdiction may hack and sell private personally identifiable information for monetary gain.

This GC panel seeks to bring a variety of perspectives to several common questions raised by this evolving new scene. What is the role for GCs with respect to cybersecurity generally? Does this change where cybersecurity issues have an international flavor? For example, how should in-house counsel interface with the third party players—not just perpetrators such as state actors—but also, on the defensive side, national security agencies and resources of the federal government, as well as international outside counsel? How should they advise their boards? What additional issues do international companies that operate 24/7 around the world face? How do they avoid or minimize operational disruption, for example, or comply fully with potentially conflicting regulatory environments, or communicate the company's cybersecurity policies effectively in different offices with different cultural and business norms?

Come learn from our esteemed panel of GCs on their insights, what they are doing, and how you might be a valuable resource to them.

Moderator:
Full Name, *Employer*

Speakers:
Full Name, *Employer*
Full Name, *Employer*
Full Name, *Employer*

International Cybersecurity

Issues and Information

Article I. Role of In-House Counsel

Section 1.01 Advising the Board

(a) Board of Directors' Fiduciary Duties

(i) Failure to implement and monitor safety and performance of cybersecurity program may expose D&O to liability in, e.g., shareholder derivative suits

(ii) No federal statutes, but some sector-specific and state requirements--for organization to implement cybersecurity measures (GLBA, HIPAA, FTCA, etc.). Some may, in certain cases, provide for extraterritorial jurisdiction

(b) Crisis Management

(c) Cybersecurity Ethics

Section 1.02 Legal Department

(a) Holistic, proactive approach

(b) Prior to any breach, GC should take active role, essentially quarterbacking all appropriate departments

(c) In case of breach, GC coordinates with relevant departments, coordinates crisis management communications, and advises board and implements its decisions

(d) Hire necessary specialized skillsets and tools (e.g., data analytics); legal budget increase justification

(e) Legal budget increase well justified

(f) Departmental systems; virtual in-house lawyers; outside counsel cybersecurity

Section 1.03 Supporting Departmental Clients

(a) Chief Executive Officer

(i) All aspects, including corporate governance and company structure

1) See, e.g., NY's Cybersecurity Regulation requires covered financial institutions to designate a CISO

(b) Chief Information Security Officer

(i) In smaller companies, GC may functionally act as CISO, at least for Board communications

(ii) Technical competence required to provide competent legal advice

(iii) New ways to communicate; new devices (e.g., Internet of Things); Artificial Intelligence

(iv) New cybersecurity tools worldwide

(v) Country-based Internets?

(c) Chief Information Officer

(i) Different technical competence; different but related issues

(d) Chief Operations Officer

(i) Contingency and Response Planning

(ii) Procurement

(iii) Regulatory compliance

(e) Chief Marketing Officer

(i) Regulatory compliance, e.g., international privacy compliance

Article II. General Cybersecurity Issues

Section 2.01 Growing and Constantly Evolving Threats

(a) Breaches Constantly Make Headlines

(i) Not IF, but WHEN

(b) High Cost to Brand

(i) Uninsurable

(c) Cybercrime Losses

(i) Est. to be $3 trillion in 2020 → 300% increase over 2016

(ii) Response costs

1) Investigation
2) Fixes
3) Breach Notification
4) Ongoing

(d) Litigation

(i) Class action

(ii) Securities litigation

(iii) FTC/DOJ

(e) Government investigations

(i) SEC

(f) Evolving Technologies

(i) Internet of Things (IoT)

(ii) Data Encryption

(iii) Social Engineering made more effective by new technologies

Section 2.02 Protection - Risk Mitigation

(a) Protection Planning

(i) Identifying Threat Vectors

1) E.g., social media; phishing; internal resources (employees); state actors; etc.

(ii) Incident Response Plan

1) Some industries, such as financial, are required to have incident response programs. See, e.g., Interagency Guidelines Establishing Information Security Standards; see also NY's Cybersecurity Regulation

(iii) Company Policies – need to be more sophisticated and customized, and compliant with applicable employment (privacy and whistleblowing) laws

(iv) Agreements – comprehensive, coordinated and customized

(v) Vendors – large % of breaches from vendors; can delegate functions, but not liability

(vi) Insurance Coverage

(vii) Coordinated planning for company offices and facilities worldwide

(b) Training

(i) Prophylactic – communicating company policies; best practices; periodic review and update

(ii) Response drills (practice)

Section 2.03 Responses to Cyberattacks

(a) General

(i) Investigation

(ii) Fixes

(iii) Breach Notification, including government reporting, where applicable; public disclosure of material data breaches by publicly-traded companies

1) Public relations
2) Working with insurance companies

(iv) Sector- and state-specific records retention requirements; general litigation hold

(v) Ongoing

(b) Worldwide crisis management

(i) Added complexity; coordination

(ii) GDPR requires 72-hours breach notification

Section 2.04 Evolving Legal Landscape

(a) Privacy Regs

(i) Possible new federal privacy law, could be game-changing

(ii) For reporting companies, see SEC's Interpretive Statement and Guidance on Public Company Cybersecurity Disclosures, rel. Feb. 2018; see also SEC's Regulation S-P (Safeguards Rule) and Regulation S-ID (Red Flags Rule)

(iii) State –constant change, mostly by accretion

(b) Operational Issues

(i) New company products and services raise new legal issues

1) E.g., IoT products—as a fitness device gathers more personal data, does it become a medical device?

(c) Federal Legislation

(i) Every day cybersecurity issues occupy a growing share of the Congressional agenda

1) See Congressional Research Service, "Transportation Security: Issues for the 116th Congress," updated Feb. 11, 2019
2) See Congressional Research Service, "Cybersecurity: Selected Issues for the 115th Congress," dated March 9, 2018 (https://news.usni.org/2018/03/27/report-congress-cybersecurity)
3) See Congressional Research Service, "Cybersecurity Issues and Challenges: In Brief," dated Aug. 12, 2016
4) See Congressional Research Service, "Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation," dated Dec. 12, 2014

(d) New Court Cases

(i) New laws and new technologies presenting novel issues will drive new precedents

Article III. International Issues

Section 3.01 National Security

(a) Broad Federal Government Involvement

(i) OMB issued memorandum M-19-23, dated July 10, 2019, re appointment by each federal agency of a Chief Data Officer ("CDO"); each agency shall also establish a Data Governance Body chaired by its CDO; and all CDOs will comprise a Chief Data Officer Council.

(ii) Department of Homeland Security

1) According to DHS, it "works with key partners across the Federal government, State and local governments, industry, and the international community to identify and manage national cybersecurity risks."
2) DHS published its "Cybersecurity Strategy" paper, May 15, 2018, re its 5-pillar approach: risk identification; vulnerability reduction; threat reduction; consequence mitigation; and enabling cybersecurity outcomes. In broad terms, this is similar to the GC's outlook and charge, and thus may be illustrative of general approaches from which GCs may learn

(iii) Department of Defense

(iv) Department of the Treasury

(v) Department of Commerce

(vi) CFIUS and FIRRMA

(vii) FARs and DFARs

(viii) OFAC

(b) Persistent Engagement

(i) National Security Agency – headed by Gen. Paul Nakasone, Director

(ii) U.S. Cyber Command

Section 3.02 Country-Sponsored Cyber-Hacking and Cybercrimes

(a) Foreign Espionage Act

(i) Criminal Sanctions

(ii) Civil Remedies and Recourse

(b) Civilian Offensive Protections

(i) Using company systems to punish intruders and other bad actors

(ii) Working with the government(s)

(iii) Government and Industry coordination and information sharing—multilateral and international

1) See, e.g., Cybersecurity Information Sharing Act – private entities may voluntarily share cyber threat indicators and defensive measures with certain government and quasi-government authorities

Section 3.03 Regulating Exports and "Deemed Exports" of Information and Technology

Section 3.04 Regulating Cross-Border Investments

Section 3.05 Special Issues for Companies with Products/Services for Children

Section 3.06 Changing Governance Structure(s) of [the] Internet(s)

Section 3.07 International Risk Mitigation

(a) Protection Planning

(i) Compliance with local country/countries laws

(ii) Company Policies – again, localize for multiple languages, cultures

(iii) Agreements – choice of law; venue; arbitration versus local court dispute resolution

(iv) Insurance Coverage – worldwide territory

(v) Coordinated planning for company offices and facilities worldwide

(b) Training

(i) Prophylactic – communicating company policies; best practices; periodic review and update

(ii) Response drills (practice)

(iii) Coordinated training for company offices and facilities worldwide

Section 3.08 Responses to Cyberattacks

(a) International

(i) Worldwide crisis management

Section 3.09 Evolving Legal Landscape

(a) Privacy Regs

(i) International

1) GDPR

a) Potential fines of 4% of annual turnover

b) 72-hour breach notification requirement

c) Data transfers outside the EU: Adequacy Declarations

i) U.S. and EU-U.S. Privacy Shield framework; Japan and South Korea – negotiations; draft adequacy decision

2) China's Cybersecurity Law, adopted June 1, 2017, re:

a) analysis of cybersecurity programs;

b) data storage within China requirements;

c) data transfers out of China; and

d) requirement to share certain cybersecurity information with Chinese government

3) India - Ministry of Electronics and Information Technology published, on 27 July 2018, the Personal Data Protection Bill and the Data Protection Committee Report re data protection obligations, including, grounds for processing personal data and sensitive personal data, personal and sensitive data of children, data principal rights, transparency, accountability measures and transfer of personal data outside India

4) Different laws, but even where same or similar, common concepts—such as consent—may differ from region to region and country to country

(ii) Possible new federal privacy law, could be game-changing

(iii) State –constant change, mostly by accretion

(b) Operational Issues