Vinson&Elkins

NOVEMBER 1, 2018

CYBER-GOVERNANCE: LEGAL CONSIDERATIONS FOR CYBER DISCLOSURE AND PREPAREDNESS

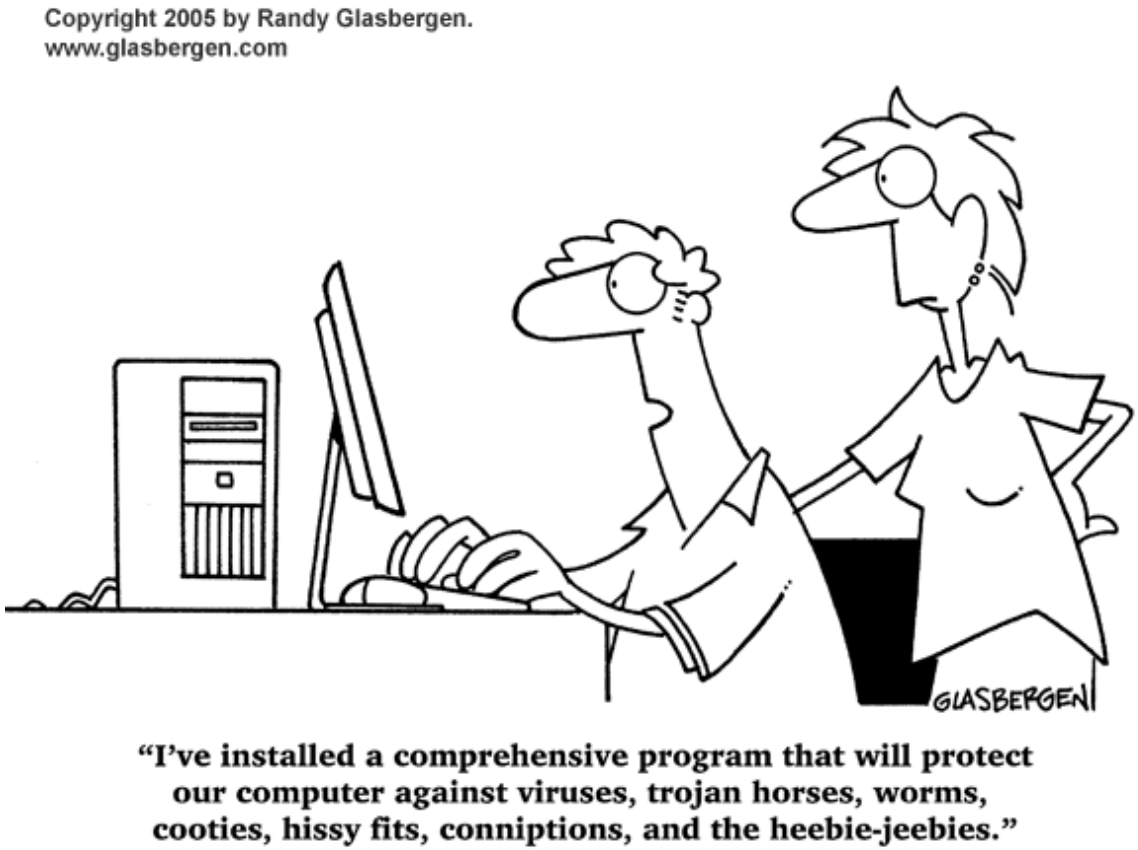
Devika Kornbacher
Sarah Fortt

DISCUSSION TOPICS

REFRESHING THE CONVERSATION ON CYBER

REFRESHING THE CONVERSATION ON CYBER

- Amid growing information, regulation and stakeholder demands regarding cybersecurity and data protection, in-house legal personnel are justified in feeling cyber-exhausted.
- Yet, cyber risks continue to multiply and expand, and stakeholders' demands for disclosure continue to grow. ***So what should companies do?***



REFRESHING THE CONVERSATION ON CYBER

- ***Keep it simple***; ***focus on key steps***:
  - Understand the **legal landscape**, including the **potential costs** associated with cyber and data incidents;
  - Tick through your **cyber to-dos**:
    - **Identify** risks;
    - **Adopt** effective policies, procedures and protections;
    - **Monitor**, **test** and **audit** your policies, procedures and protections and implemented **controls**;
    - Create effective **disclosures**; and
    - **Plan** for breach/attack.
  - Keep the **board** up to date.

CONCEPT OF CYBERSECURITY/DATA PRIVACY

THE DIFFERENCE BETWEEN CYBERSECURITY AND DATA PRIVACY

- **Cybersecurity**: Keeping information on computer systems and networks safe, available, and accurate
- **Data Privacy**: Collection, use, storage, and disclosure of personal data in a manner that ensures confidentiality, integrity, and limited exploitation of the data while providing the person appropriate control over such activities
- **Cybersecurity** + **Notice, Consent, Etc.** = **Data Privacy**

EQUIFAX®

Equifax Announces Cybersecurity Incident Involving Consumer Information

Facebook, Cambridge Analytica face lawsuit over privacy loss

BY **STEPHEN SHANKLAND** / MARCH 22, 2018 12:37 PM PDT

THE EXPONENTIAL GROWTH OF TOTAL DATA

WHY IT IS IMPORTANT TO IMPLEMENT PROPER CYBER HEALTH NOW

2020

*Total data is expected to increase by 50x from 2010 to 2020.**

** The Intelligent Use of Big Data on an Industrial Scale; insideBIGDATA, LLC; Hewlett Packard Enterprise (2017).*

THE EVOLVING LEGAL LANDSCAPE

THE EVOLVING LEGAL LANDSCAPE

U.S. CYBERSECURITY/DATA PRIVACY LAWS AND REGULATIONS

- The Securities and Exchange Commission recently issued Cybersecurity Disclosure Guidance and several recent SEC enforcement actions have focused on flawed or failed cyber controls.

- Per the Health Insurance Portability and Accountability Act (HIPAA), the Department of Health and Human Services has established information security standards for the handling of Protected Health Information.

- Section 5 of Federal Trade Commission Act prohibits unfair and deceptive trade practices.

THE EVOLVING LEGAL LANDSCAPE
RECENT SEC ENFORCEMENT ACTIONS

- ***The SEC charged Voya Financial Advisors Inc. with deficient cybersecurity procedures***. Specifically, the SEC charged Voya with violating the Safeguards Rule and the Identity Theft Red Flags Rule, which are designed to protect confidential customer information and protect customers from the risk of identity theft. According to the SEC's September 2018 order, pursuant to which Voya agreed to settle charges in exchange for a $1 million penalty, Voya's failure to terminate intruders' access to its systems stemmed from weaknesses in its cybersecurity procedures, some of which had been exposed during prior similar fraudulent activity. According to the order, Voya also failed to apply its procedures to the systems used by its independent contractors.

- ***Earlier this year, the SEC announced that the entity formerly known as Yahoo! had settled charges that it failed to disclose its cybersecurity breach***. Yahoo! agreed to pay a $35 million penalty to settle the charges that it misled investors by failing to disclose one of the world's largest data breaches, in which hackers stole personal data relating to hundreds of millions of user accounts.

THE EVOLVING LEGAL LANDSCAPE

U.S. CYBERSECURITY/DATA PRIVACY LAWS AND REGULATIONS

- Massachusetts and New York prescribe minimum security standards.
- California recently passed the **Consumer Privacy Act**, which requires all businesses dealing with data of California residents to implement and maintain reasonable security procedures. It also grants California residents the right to request record of PII, deletion of PII, details of PII disclosures, and opt out of a sale of PII.
- While there currently is no comprehensive federal data breach notification law, all 50 states and some U.S. territories have breach notification laws.

- **EU General Data Protection Regulation (GDPR)**
  - Replaced Data Protection Directive as of **May 25, 2018**
  - "**Personal Data**" is any information relating to an identified or identifiable natural person
  - Requires that each Member State protect its peoples' fundamental rights to data privacy and prohibits the transfer of personal data to any country outside the EU that does not "ensure an adequate level of protection." [Article 45]
    - Only the laws of 11 countries provide this "adequate level of protection"
    - The U.S. is not one of the 11 (but EU-U.S. Privacy Shield intended to allow transfers)

THE EVOLVING LEGAL LANDSCAPE
EU GENERAL DATA PROTECTION REGULATION, CONT'D

- ***GDPR Applicability***: "processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."
- ***GDPR Fines***: Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher.
- **Obligations depend on role (i.e. controller, processor)**.

THE EVOLVING LEGAL LANDSCAPE

GDPR: LAWFUL BASIS FOR PROCESSING

- Data subject has given consent. Consent must be freely given, specific, informed, and unambiguous. Consent must also be by a statement or clear affirmative action (demonstrable), clearly distinguishable from other matters, intelligible form, easily accessible, in clear & plain language. The data subject must have an easy right to withdraw and must be informed of this right when consent is provided.
- Processing is necessary for the performance of a contract to which the data subject is party.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for legitimate interests pursued by the controller or by a third party.

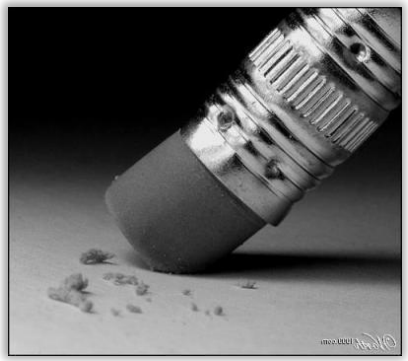
- **Transparency Notices:**

  - Clearly communicate rights of data subject in writing
  - When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means
  - Within one month of data subject's request, provide description of all actions taken with subject's personal data, free of charge
  - Includes communications regarding a breach

- **Access Requirement:** Data subject has right to:
  - Confirmation of processing
  - Access to personal data
  - Access to categories of personal data concerned
- **Portability Requirement**: Data subject has right for data:
  - In a structured, commonly used and machine readable format, to be transmitted to another controller (w/o hindrance) directly from one controller to another;
  - If processing is based on consent or performance of contract, and carried out by automated means

THE EVOLVING LEGAL LANDSCAPE
EU GENERAL DATA PROTECTION REGULATION, CONT'D

- **Right to be Forgotten:** Data subject has right to erasure of data if:
  - Data is no longer necessary for purpose
  - The data subject withdraws consent and there is no other legal ground for the processing
  - The data subject objects to processing and there is no overriding legitimate grounds for the processing
  - Data has been unlawfully processed
  - Necessary for compliance with another legal obligation
- **If controller has made data public, then they must take reasonable steps to inform other controllers**
- **Exceptions to Right to be Forgotten:**
  - Freedom of expression (e.g., journalistic purposes)
  - Legal obligation or defense of legal claims
  - Public interest



THE EVOLVING LEGAL LANDSCAPE
INTERNAL AND THIRD PARTY OBLIGATIONS AND INDUSTRY STANDARDS

- **Duties to protect employee data** (*See*, *e.g.*, *Michael Corona, et al v. Sony Pictures Entertainment, Inc.,* No. 14-CV-09600, filed March 2, 2015 (C.D. Cal.))
- **Obligations of officers and directors to manage risk** (e.g., corporate duty of due care)
- **Privacy and data use/collection policies**
- **Payment Card Industry Data Security Standard (PCI-DSS)**
- **Audit and accounting requirements** (apply to data integrity and accuracy)
- **Contractual commitments**
- **Common law obligations to third party data owners**
  - No negligence
  - Confidentiality obligations
  - Implied contract
  - Duty of good faith
- **Insurance requirements**

EXTERNAL STANDARDS AND FRAMEWORKS

- Commonly accepted frameworks and guidance for cybersecurity programs:

  - The **National Institute of Standards and Technology** (NIST) voluntary Framework for Improving Critical Infrastructure Cybersecurity (2018)

  - The **International Organization for Standardization** (ISO) ISO/IEC 27001 requirements for an information security management system (2013)

  - **DOJ Guidance** on “Best Practices” for Cyber-Incident Response Plan (Apr. 2015)

  - **Department of Energy** issued “Energy Sector Cybersecurity Framework Implementation Guidance” for implementation of NIST Framework (Jan. 2015)

THE POTENTIAL COSTS OF A CYBER/DATA INCIDENT

Direct Costs

- Litigation (e.g., stakeholder, consumer)
- Enforcement (e.g., SEC, state regulator, CFPB)
- Breach notification
- Regulatory fines
- Investigation
- Remediation

Indirect Costs

- Stock price
- Higher customer churn
- Loss of IP/competitive advantage
- Reputational harm

CYBERSECURITY PRACTICE POINTS

CYBERSECURITY PRACTICE POINTS
CYBER RISK IDENTIFICATION

- **Common types of data security events:**
  - Unintended disclosure (public website post, emailed wrong person, social engineering/phishing scam);
  - Hacking (electronic entry by an outside party or malicious software);
  - Malicious insider; and
  - Physical loss (lost or stolen mobile devices, etc.).
- **Cyber events can result in:**
  - Distributed denial of service (DDoS);
  - Ransomware attack; and
  - Other data leakage.

CYBERSECURITY PRACTICE POINTS
CYBER RISK IDENTIFICATION

Process	Key Questions	Cyber/Data Considerations
Risk Identification	▪ Are cyber risks identified as a part of the ERM process or separately? ▪ How does the company define materiality in the cyber context? ▪ What criteria and procedures does the company use to identify and report cyber risks internally? ▪ How often are cyber risks identified and how does the company assess the process for identification? ▪ Has the company solicited outside help in this process?	A company that is assessing the materiality of cybersecurity risks is unlikely to be able to fully assess the magnitude of the potential costs associated with each cyber-event. Therefore identifying the range of potential events, and the company's exposure to those events, is critical. Outside consultants can be very helpful in completing this process. For cyber matters, the risk identification process needs to encompass the entire organization, as well as third parties.

COMPREHENSIVE INFORMATION SECURITY PROGRAM
EFFECTIVE POLICIES, PROCEDURES AND PROTECTIONS

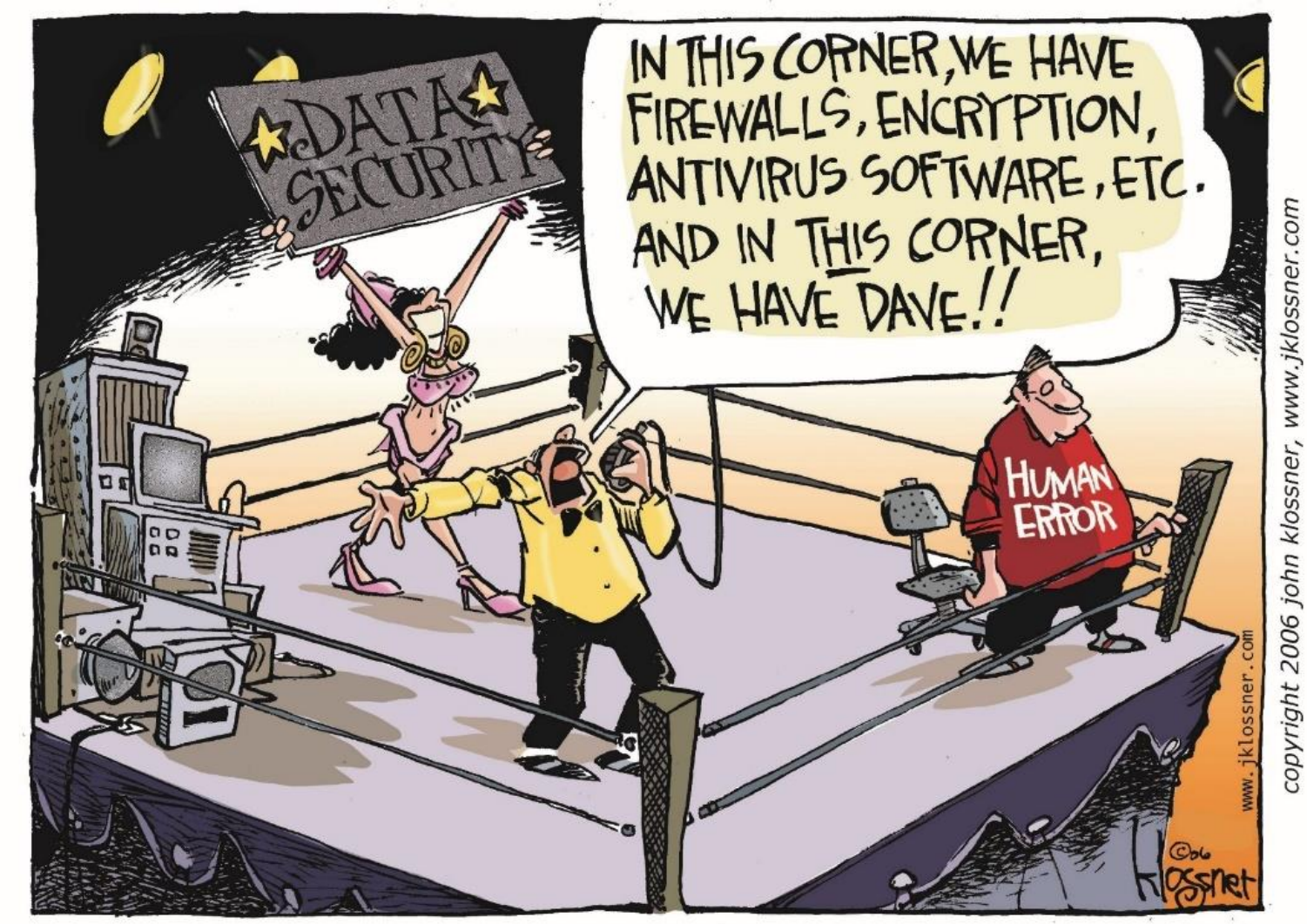
Process	Key Questions	Cyber/Data Considerations
Policies, Procedures and Protections	▪ What cyber and data policies, procedures and protections has the company put in place, and why is the company confident that those comprise the right approach? ▪ Has the company considered the cyber implications of its other policies (e.g., insider trading, code of conduct)?	Policies, procedures and protections should be informed by the risk assessment process, but tested and revised accordingly. Companies should consider whether to revise internal or public policies to specifically address trading and ethical implications in the cybersecurity context.

COMPREHENSIVE INFORMATION SECURITY PROGRAM
EFFECTIVE POLICIES, PROCEDURES AND PROTECTIONS

- **Policies, procedures and protections should:** Clearly **identify** risk areas, help **detect** potential issues, help **protect** against breaches and attacks, **detect** gaps and weaknesses in the network and in controls, tell persons how to **respond** to any potential issue, **preserve** evidence and **protect** the company's data, and help **recover** any lost information.
- **Cover all bases:**
  - Digital (e.g., multi-factor authentication);
  - Physical (e.g., off-site redundancy); and
  - Human (e.g., chief information security officer (CISO)).
- **Policies, procedures and protections are only as good as the implementation and education!**

COMPREHENSIVE INFORMATION SECURITY PROGRAM

EDUCATION AND TRAINING - PLANNING FOR DAVE



COMPREHENSIVE INFORMATION SECURITY PROGRAM
EDUCATION AND TRAINING - PLANNING FOR DAVE

- ***A company's number one source of cyber risk is usually its employees*.**
- The recent 2018 Industry Report by Shred-It, an information security company, indicates that employee negligence is a main source of cyber breaches and related risks. ***So what can a company do?***
- ***Training***. Employee training is probably the most important part of a company's cybersecurity and data protection efforts. It is not enough to distribute a policy once a year. In-person and hands-on training programs, and phishing tests should be done regularly.
- ***Review access regularly***. Companies should review whether the access employees have is appropriate; and don't forget to terminate/update access for employees who leave or move.
- ***Reduce and dispose of information appropriately***. Subject to the need to retain certain information for legal reasons, companies should reduce and appropriately dispose of information appropriately and regularly.
- ***Communicate key contacts***. Make sure employees know who to call if they suspect the company's networks or data have been compromised.

COMPREHENSIVE INFORMATION SECURITY PROGRAM
MONITOR AND TEST

Process	Key Questions	Cyber/Data Considerations
Monitor and test	▪ How does the company monitor and review the effectiveness of the processes for identifying and mitigating cyber risks? ▪ What tests does the company conduct to review effectiveness?	While many companies have security measures and internal trainings, companies should consider how these efforts function throughout the organization and whether it has the right processes and conversations in place.

COMPREHENSIVE INFORMATION SECURITY PROGRAM
MONITOR AND TEST

- Companies that have comprehensive info-sec programs:
  - Periodically run **penetration testing** conducted by an outside specialist;
  - Evaluate **third parties**' cybersecurity efforts (e.g., review their audit reports);
  - Conduct **"phake phishing"** and similar tests to assess the effectiveness of employee training;
  - Conduct **trial runs** of incident response plans (e.g., table-top exercises) conducted by outside specialist;
  - Use **other internal reporting mechanisms** to assess whether employees will report any identified issue (e.g., compliance hotline records);
  - Conduct **traditional** monitoring (e.g., cameras and access logs); and
  - Conduct **technological** monitoring (e.g., managed security services).

COMPREHENSIVE INFORMATION SECURITY PROGRAM
AUDIT AND CONTROLS

Process	Key Questions	Cybersecurity Considerations
Disclosure	▪ How does the company assess whether 10-K/10-Q disclosure is needed? ▪ What 8-K cybersecurity disclosure controls are in place?	In addition to evaluating existing cyber-related risk factors, companies should consider (i) whether the costs associated with cybersecurity efforts have or will become material, (ii) whether it makes sense to discuss the board's oversight of cybersecurity matters in the risk oversight section of the proxy statement, and (iii) whether 8-K controls adequately address cyber matters.
Evaluation	▪ How does the company assessed its approach to each of these steps?	An effective cybersecurity program includes evaluation of each aspect of the program, including pressure testing and simulation of cyber events.

COMPREHENSIVE INFORMATION SECURITY PROGRAM
AUDIT AND CONTROLS

- Companies that have effective information security programs:
  - Regularly review its **cyber disclosure** if a public company. An effective program will regularly review whether the company's cyber disclosure is **transparent**, **thoughtful**, and **complete**.
  - Conduct **audits**. Audits may include Statement on Standards for Attestation Engagements No. 18 SOC-2, NIST, ISO, PCI-DSS, HIPAA, etc.
  - Adopt **disclosure controls** (e.g., when does a cyber event need to be disclosed).
  - Adopt **policy/procedure controls** for each part of the program (e.g., are the risk assessment, policy, monitoring/testing and reporting functions working properly).

CYBERSECURITY PRACTICE POINTS
INCIDENT RESPONSE

Process	Key Questions	Cyber/Data Considerations
Incident Response Plan	▪ What is the company's definition of a cybersecurity "event"? ▪ How/when are issues escalated? ▪ Who is on the response team? ▪ What are the communication plans?	Upper management should endorse the plan and be involved. An effective response plan addresses (i) escalation, (ii) the response plan team, including any outside advisors, and (iii) internal and external communications.

CYBERSECURITY PRACTICE POINTS
INCIDENT RESPONSE

Incident Response Checklist:

- ❑ Contact outside counsel to put activities under scope of attorney-client privilege
- ❑ Initiate incident response plan, including call tree
- ❑ Determine breadth, origin and nature of incident and whether it is an actual breach/attack
- ❑ Determine the type and scope of data compromised, as well as the devices and systems affected
- ❑ Review cybersecurity insurance policies and notify carrier (*some policies require notice as short as 3 days from discovery)*
- ❑ Don't reimage or delete files; preserve all evidence
- ❑ Order a litigation hold, if prudent
- ❑ Develop uniform message for communications, including an appropriate description of the breach and compromised data
- ❑ Notify state, federal, or foreign entities as required
- ❑ Notify affected users as required
- ❑ Prepare for defense of third-party claims and governmental investigations
- ❑ Review and revise internal policies as necessary to document lessons learned
- ❑ Contact law enforcement, if appropriate
- ❑ Perform analysis of state, federal and foreign breach notification requirements for every data type compromised

CYBERSECURITY PRACTICE POINTS
INCIDENT RESPONSE TEAM

Position	Internal Member(s)	External Counterpart(s)
Information Technology ("IT")	• Chief Information Security Officer (if the CISO sits within IT) • IT Management Personnel	• Technical Forensics Consultant • Co-location Facilities Contact
Legal and Compliance	• General Counsel or Designee • Privacy Officer • Chief Information Security Officer (if the CISO sits within legal or compliance) • Human Resources Personnel	Outside Counsel
Business Management	• Chief Executive Officer, Chief Information Officer or Designee • Board Liaison	Outside Counsel
Public Relations	Chief Marketing Officer or Communications Manager	Public Relations Firm
Risk Management	Risk Management Specialist	Insurance Consultant

KEEPING THE BOARD INFORMED

INFORMING THE BOARD: BOARD MATERIALS

- Comprehensive information is critical for directors to meet their duty of care. Effective materials can also help protect the company from liability.

- ***Quantity***. Generally, boards should receive enough information so that they can make informed decisions, but not so much that the volume obscures what is most relevant. For this reason, members of management reporting up to the board should be encouraged to summarize and prioritize their information, and clearly identify takeaways and action items.

- ***Purpose***. Directors should always understand *why* they are being provided with the information. Those reporting to the board should be encouraged to define the purpose of the information: Is it to (1) equip the board to make decisions about the company's future (and what are those decisions)? (2) inform the board about the company's past performance? (3) notify the board of a concern or issue that must be addressed? (4) educate the board on matters of general relevance to the company?

INFORMING THE BOARD: BOARD MATERIALS

- ***Types***. The types of information the board should receive include anything that is material to their oversight of the company's strategy, management, compliance with legal requirements, and operations. Information regarding the CEO's performance, certain legal, ethical and compliance-related matters, and other governance matters is required to be submitted to the board to comply with SEC and exchange rules.

- With limited exception, materials should not be retained by directors following a board meeting, and directors generally should avoid taking personal notes regarding meeting matters.

CHALLENGES OF INFORMING THE BOARD

Common Complaints

***Board materials are too long*.**

***Board materials take too long to prepare*.**

***Unclear whether the board is receiving the right types of internal information*.**

***Lack of third-party information*.**

***Board materials are inconsistent in approach*.**

***Board materials are difficult to understand*.**

***Unclear what the purpose of the information is and whether any follow up is needed*.**

Good Practices

- Include a one page summary with key takeaways and to-dos.
- Regularly assess the materiality of details being included.
- Make sure the board receives good and bad news.
- Include reports/articles from outside experts.
- Establish a template for those reporting to the board to follow.
- Use plain English and cross-check materials across business units.
- Always identify why materials are being provided and whether/what board action is needed.

KEY BOARD QUESTIONS FOR CYBER OVERSIGHT

Questions to Assist Directors in Assessing the Adequacy of Cybersecurity
Who is the senior person with clear responsibility for company-wide cybersecurity preparedness?
How is access granted and reviewed? How is the appropriate level of access determined? How quickly is access terminated for former employees?
How does the company detect and respond to attempted attacks or potential breaches?
How are employees trained on prevention and reporting of suspected cybersecurity breaches?
To what degree is management comfortable that the company has effectively protected itself against intentional or inadvertent employee-created vulnerabilities?
How does the company's cyber-readiness compare to its peers?
How does management assess the adequacy of its technological measures for preventing, detecting and responding to cybersecurity breaches?
How does management assess the safety of sensitive non-digital information?
How is cybersecurity risk management aligned with the company's overall ERM process?
How and how often does the company test its cyber-awareness and readiness?

THIS CONTENT IS INTENDED FOR EDUCATIONAL AND INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE LEGAL ADVICE OR SERVICES. IT DOES NOT CONSTITUTE THE PROVISION OF LEGAL ADVICE OR SERVICES BY ANY OF THE SPEAKERS OR BY VINSON & ELKINS LLP.

Austin
T +1.512.542.8400

Beijing
T +86.10.6414.5500

Dallas
T +1.214.220.7700

Dubai
T +971.4.330.1800

Hong Kong
T +852.3658.6400

Houston
T +1.713.758.2222

London
T +44.20.7065.6000

Moscow
T +7.495.544.5800

New York
T +1.212.237.0000

Richmond
T +1.804.327.6300

Riyadh
T +966.11.250.0800

San Francisco
T +1.415.979.6900

Tokyo
T +81.3.3282.0450

Washington
T +1.202.639.6500

SPEAKER PROFILE

DEVIKA KORNBACHER
PARTNER, INTELLECTUAL PROPERTY

Houston / New York

+1.713.758.2757

dkornbacher@velaw.com

Education

- Harvard Law School, J.D., 2006
- University of Houston, B.S.C.E. *cum laude*, 1998

Devika leverages her background and experience to assist clients in obtaining, protecting, licensing, and enforcing intellectual property rights, with a particular emphasis on technology law in the context of mergers, acquisitions, investments, project development and day-to-day business transactions. She counsels clients in fields such as energy, sports, aviation, software and hardware on digital media, open source software, cybersecurity, and other technology matters. She also has experience with a wide-array of transactions, including commercialization agreements, license agreements, reseller arrangements, collaboration agreements, joint ventures, software development agreements, and patent clearances.

Devika has also been designated a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP) and serves as the Chair of the Firm's Cybersecurity & Data Privacy Task Force.

Representative Experience

- Advising Medicare provider with incident response following a breach that directed payment to accounts not associated with the provider
- Represented student loan collection company in defending information security risk assessment for Department of Education under Federal Information Security Management Act
- Counseled major sports league on implementation of information security program, including negotiation of agreements with security vendors
- Drafted privacy policies for multiple companies in various industries, including telecommunications, software, energy and oilfield services, real estate, social networking, transportation, and engineering
- Advised aviation company on the development of a plan (and model notices) to inform employees and/or client in the event of a data breach involving personal information
- Counseled a pharmaceutical company on open source software and cybersecurity matters in connection with its acquisition of provider of cloud-based solutions for chronic respiratory disease management
- Counseled multiple companies on compliance with the recently-effective EU General Data Protection Regulation

SPEAKER PROFILE

SARAH E. FORTT
SENIOR ASSOCIATE, MERGERS & ACQUISITIONS AND CAPITAL MARKETS

Austin

+1.512.542.8438
sfortt@velaw.com

Education

- Yale Law School, J.D., 2010 (Editor, *Yale Journal on Regulation*)
- Gordon College, B.A., Business Administration and English Literature & Language *summa cum laude*, 2004

Sarah's principal area of practice is securities law and corporate governance. She advises clients, including public companies and their boards of directors, on corporate governance, securities law and regulatory matters, including exchange listing standards. Sarah is also well versed in executive compensation best practices and disclosures. Representative matters include advising clients on Securities and Exchange Commission reporting requirements, proxy and periodic disclosures, director independence and qualification matters, proxy advisory firm policies, board and committee procedures and governance documents, shareholder engagement and corporate governance activism, and disclosure controls and procedures. Sarah is also experienced with emerging corporate governance matters including proxy access, cybersecurity risk disclosures and oversight, corporate social responsibility statements and disclosures, proxy redesign, pay-for-performance and wage parity disclosures, and political contributions disclosures. Sarah also advises non-profit organizations on corporate governance issues.

Select Experience

- Presentations to S&P 500 boards of directors on corporate governance best practices and key governance developments, including insights regarding risk oversight, crisis management, oversight of executive compensation, succession planning, board communications and materials, and stockholder communications
- Support to General Electric, Bank of America, Schlumberger, Intel, Carnival Corporation and others each in their annual preparation for their stockholders meetings', including addressing stockholder proposals, drafting and reviewing proxy statement disclosure and assisting with stockholder engagement efforts
- Business Roundtable policy statements regarding corporate governance and comment letters to the Securities and Exchange Commission on key governance developments
- Ongoing governance support for over a dozen corporations, including independence analysis, implementation of governance policies and procedures, disclosures, and board presentations
- Detailed analyses of current practices and compilation of governance recommendations for nonprofit and charitable organizations