PRESENTERS

Christopher Cwalina, Partner
Holland & Knight
Chris is a partner in Holland & Knight's Washington, D.C., office and co-chair of the Data Privacy and Security Team. He concentrates his national practice primarily on privacy and data security compliance; litigation; defending companies in investigations initiated by state attorneys general, the FTC and other government agencies; responding to security breach incidents; establishing international compliance frameworks for companies; and developing and writing company policies and procedures.

Mark Seifert, Partner
Brunswick Group
Mark has more than 15 years of telecommunications and technology policy experience. He founded Brunswick’s Corporate Data practice, where he advises major multinational corporations on the communications and reputational issues surrounding data, security, privacy, and crisis. Immediately prior to Brunswick, Mark oversaw a $5bn broadband infrastructure program at the US Department of Commerce. In addition to his time as a regulatory lawyer at the FCC, Mark also served as counsel to the House Committee on Energy and Commerce on telecommunications and technology matters.
DATA: A VALUABLE ASSET

Data is one of a company’s most valuable assets, but it also represents a significant risk. Corporate reputation is now judged, in part, on a company's responsible stewardship of its data, so corporate leaders need to take reasonable measures to protect this asset.

In the application process alone, the Multifamily Housing industry regularly collects sensitive data for millions of citizens. That data is valuable and everyone knows you have it—your customers, regulators, and most recently—organized crime.
EVERYONE IS A TARGET

Adobe
CHASE
global payments
YAHOO!

Zappos
Anthem
BlueCross BlueShield

living social
The New York Times
Disney

tripadvisor
SONY
Michaels
Citizens Bank

HOME DEPOT
NASA
NASDAQ
TJ MAXX
Attacks are inevitable and adversaries are quickly evolving.

A critical part of preparedness is knowing how to respond appropriately, confidently, and accurately about a data issue.

Regulators now look at what companies have done to prepare and prevent – not just how they respond.
A RESPONSIBILITY OF THE BOARD & CEO

- Boards are being held accountable
- In June 2014, SEC Commissioner Luis A. Aguilar explicitly said that Cyber Security oversight is a Board responsibility
- The National Association of Corporate Directors recently released its first Cyber-Risk Oversight Handbook detailing steps “all corporate boards should consider as they seek to enhance their oversight of cyber risks”
CYBERTHREATS ARE NOT JUST A TECH PROBLEM

- The most successful cybersecurity programs are integrated with Enterprise Risk Management
  - Bringing business leaders, legal, compliance, and public and government relations together with technologists to understand cyber risk can pay huge dividends both in risk reduction and cost savings
- Vendors have been a critical vector for recent attacks on companies across multiple industries and sectors
  - In today’s competitive marketplace, companies frequently outsource critical functions to vendors (e.g. information technology, payment processing, etc.)
WHAT YOU NEED TO KNOW

1. Who’s attacking and why

2. Post-SONY, the stakes are even higher

3. It’s more than technology. It’s about your business processes and your people

4. Preparation and process will help reduce costs
The average data breach in the United States costs an organization more than $5.4 million.

Organizations with an “incident response plan” at the time of their breaches, tested, and were able to respond quickly, saw an average cost that was $42 per record less than the national average per compromised record.

Testing policies/procedures (in advance of an incident) demonstrates compliance focus/efforts and can inform prosecutorial discretion should an actual incident occur.

How you prepare and how you respond reduces the cost of these incidents.
WHAT YOU CAN DO

Know Your Assets & Liabilities

Establish a Breach Response Process

Understand what shapes your reaction and response

Train, Test and Evaluate
KNOW YOUR ASSETS AND LIABILITIES

For non-digital natives, make your team translate until you understand it the way you understand the dollars that flow through your organization:

- What data do you have?
- What do you do with your data?
- How do you protect data?
ESTABLISH A BREACH RESPONSE PROCESS

- Ensure you have a process and written plan that applies across all functions

- Remember that multiple response plans need to be married and work together with commonly understand definitions

- Determine clear escalations and triggers
UNDERSTAND WHAT SHAPES YOUR RESPONSE

Legal triggers for disclosure and regulatory schemes that govern the data you have

Forensic process that informs your ability to understand

Customer and public expectations directly affect your corporate reputation
TRAIN, TEST, AND EVALUATE

- Conduct training exercises with your employees
- Ensure your executives have fluency in the issues and buy into the process
FINAL THOUGHTS

Bank robbers rob banks because that is where the money is kept

Preparation is a cost reduction measure

Do not delegate this task
APPENDIX
# Legal Issues – Cybersecurity Risk

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputational Damage</td>
<td>Negative perception by customers, media, public due to publicized issues</td>
<td>Organization could experience negative publicity, lose customers, revenue, confidence and potentially be targeted by other cyber adversaries</td>
</tr>
<tr>
<td>Reduction of competitive edge with direct competitors</td>
<td>Theft of intellectual property (e.g., corporate processes, customer databases, privileged communications)</td>
<td>Customers could be contacted by competitors and entice with slightly better deals, tradecraft could be analyzed allowing competitors to adapt and alter or destroy data in databases, making it very difficult or impossible for operations to work and requiring incident response/data recovery functions to be enacted</td>
</tr>
<tr>
<td>Loss of data or systems</td>
<td>Destruction of data, systems, or access to systems through willing or accidental means; physical loss of mobile devices</td>
<td>Adversaries could alter or destroy data in databases, making it very difficult or impossible for operations to work and requiring incident response/data recovery functions to be enacted</td>
</tr>
<tr>
<td>Data breach disclosure</td>
<td>Compromise of internal integrity and public disclosure of privileged communications or customer data</td>
<td>Unauthorized disclosure of or access to personal information (e.g., PII, payment information) can not only cost an organization (response, notices, etc.), but can create a problem for customers and partners and result in liability from various angles, including government/ regulatory investigations, litigation, etc.</td>
</tr>
<tr>
<td>Loss of customers</td>
<td>Customer’s loss of confidence in services offered</td>
<td>Customers might simply leave the company for another, regardless of cost, in order to distance themselves from fallout from a catastrophic cyber incident</td>
</tr>
</tbody>
</table>
Legal Issues – Compliance Risk

Federal Government Actions/Investigations
- Congress
- FTC
- OCR

State Government Actions/Investigations
- Anthem
  - Less than a week after breach publicly confirmed, at least 6 state AG investigations as well as National Association of Insurance Commissioners and California Department of Insurance
- Target
  - CT AG sent inquiry same day breach publicly confirmed and requested information within 3 weeks
- Kaiser
  - CA AG brought action, arguing Kaiser took too long to provide notice of security incident (3 months after forensics; ~1 month after contents inventory)
  - Settlement – Kaiser must provide notification on “rolling basis” and must notify as soon as individuals are identified, even if investigation ongoing

Private Actions
Legal Issues – Best Practices & Recommendations (Documentation)

Written Information Security Plan

- Incident Response Plan

Identify procedures for cross-functional communication, engagement, and escalation

Ensure all relevant parties are “at the table”

- Senior Executives
- Information Technology
- Information Security
- Legal
- Privacy/Compliance
- Public Relations
- Government Relations
- Marketing
- Business Units
Legal Issues – Best Practices & Recommendations (Contracts)

Contracts that enable effective vendor risk management

- Minimum requirements for security controls, log retention, incident response cooperation (consistent with your own policies/requirements)
- Explicit treatment of regulatory requirements and the vendor’s responsibilities for compliance
- Audit rights that enable you to conduct regular (annual) on-site audits of the vendor’s policies, processes and controls
- Adjudication process for resolving concerns that are identified as a result of those audits
- Requirements for participation in cyber risk management activities including training, exercises, information sharing, breach notification
CONTACT INFORMATION

Christopher Cwalina, Partner
Holland & Knight
Co-Chair, Privacy and Data Security Team
800 17th Street, NW, Suite 1100 | Washington DC 20006
Tel. (202) 469 5230
chris.cwalina@hklaw.com | www.hklaw.com

Mark Seifert, Partner
Brunswick Group
Brwnswick Group LLC
1099 New York Avenue, NW | Washington, DC 20001
Tel. (202) 393 7337
mseifert@brunswickgroup.com | www.brunswickgroup.com