TIPS FOR FORGING A BETTER WORKING RELATIONSHIP BETWEEN COUNSEL AND IT TO IMPROVE CYBER-RESPONSE

Association of Corporate Counsel NYC Chapter | 11/1 | NYC
MEET THE PRESENTERS

GEORGE SOCHA - MODERATOR
Managing Director, BDO

PATRICK J. BURKE
Senior Counsel, Seyfarth Shaw

IAN LEWIS
Director, BDO

RACHEL MILLER
Vice President, Legal Affairs, Technology, HBO
AGENDA

I. COSTS OF CYBER INCIDENTS
II. PERSPECTIVES FROM IT
III. PERSPECTIVES FROM LEGAL
IV. Q&A
COSTS OF CYBER INCIDENTS
A CYBER INCIDENT OCCURRED. WHAT ARE THE COSTS?

REPUTATIONAL HARM
- Loss of intellectual property or records fundamental to the viability of the business/organization
- Business interruption costs
- Loss of revenue

OPPORTUNITY COST (FUTURE BUSINESS AND TALENT, INDEFINABLE)
- Increased cyber insurance cost
- IT Infrastructure restoration costs
  - Hardware / Software replacement costs
- Cybersecurity costs related to securing data and the network
  - Information security hardware, software and services
  - Compliance with HIPPA, PII and PCI standards
- Regulatory scrutiny and adverse action
  - Civil liability and class action suits
  - Fines and sanctions
  - Ponemon Institute / IBM study 2016 cost of a breech per record
    Average: $158 (Healthcare $355, Retail $172, Transport $129)
A CYBER INCIDENT RESPONSE: A MULTI DISCIPLINE CORPORATE RESPONSE WILL BE REQUIRED

- Information Security
- Information Technology
- Legal
- Risk
- C-Suite and Board
- Compliance
- Audit
- Public Relations

- Internal Communications
- Human Resources
- Finance
- Government Relations
- Continuity of Operations
- Security/Investigations
- Logistics, Transportation
COSTS OF CYBER INCIDENTS

NEW PRESIDENTIAL CYBER DIRECTIVE / PPD-41

- To provide greater clarity about the Federal government’s role in a major cyber incident
- Designated lead agencies for government action, broken into three categories:
  1. Responding to the threat (Investigation - FBI and Cyber Task Force)
  2. Protecting the organization’s assets and restoring operations (DHS)
  3. Intelligence gathering and analysis (CTIIC - for government)
- Principles to guide the government’s response to a cyber incident, emphasizing the importance of shared responsibility and coordination.
- Unified Coordination Group (UCG)
- A shared framework for evaluating and assigning a level of severity to a cyber incident (Severity Schema)
- Victim of a breach is a victim of crime
- Cooperation and information sharing with the private sector is essential to defending the nation against cyber threats
### PPD-41 SEVERITY SCHEMA

<table>
<thead>
<tr>
<th>Level</th>
<th>Color</th>
<th>General Definition</th>
<th>Observed Actions</th>
<th>Intended Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 5</td>
<td>Emergency (Black)</td>
<td>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov’t stability, or to the lives of U.S. persons.</td>
<td>Effect</td>
<td>Cause physical consequence</td>
</tr>
<tr>
<td>Level 4</td>
<td>Severe (Red)</td>
<td>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</td>
<td>Presence</td>
<td>Damage computer and networking hardware</td>
</tr>
<tr>
<td>Level 3</td>
<td>High (Orange)</td>
<td>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</td>
<td>Engagement</td>
<td>Corrupt or destroy data</td>
</tr>
<tr>
<td>Level 2</td>
<td>Medium (Yellow)</td>
<td>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</td>
<td></td>
<td>Deny availability to a key system or service</td>
</tr>
<tr>
<td>Level 1</td>
<td>Low (Green)</td>
<td>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</td>
<td>Preparation</td>
<td>Steal sensitive information</td>
</tr>
<tr>
<td>Level 0</td>
<td>Baseline (White)</td>
<td>Unsubstantiated or inconsequential event.</td>
<td></td>
<td>Commit a financial crime</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Nuisance DoS or defacement</td>
</tr>
</tbody>
</table>

- **Effect**
  - Cause physical consequence

- **Presence**
  - Damage computer and networking hardware

- **Engagement**
  - Corrupt or destroy data

- **Preparation**
  - Steal sensitive information

- **Consequence**
  - Deny availability to a key system or service

- **Engagement**
  - Steal sensitive information

- **Preparation**
  - Commit a financial crime

- **Consequence**
  - Nuisance DoS or defacement
COSTS OF CYBER INCIDENTS

CYBERSECURITY PRE- & POST-INCIDENT RESOURCES

- Independent Risk Assessment
- Remediation Implementation
- Penetration Testing
- Social Engineering Testing
- Network Architecture
- Cost Optimization
- Technology Optimization
- Employee Training
- Strategic Board Advisory Services
- Incident Response Planning
- Cyber Insurance Review and Purchase Assistance
- Digital Asset Valuation
- Data Mapping
- Network Mapping
- Incident Response
  - Containment
  - Mitigation
  - Recovery
  - Continuity of Business Operations
  - Investigation
  - Forensics
  - Vulnerability Assessment
  - Government Relations
  - Strategic and Board Advisory Services
  - Media and Legal
IMPORTANT ASPECTS OF A MATURE GOVERNANCE PROGRAM - LESSONS LEARNED

- Things will happen when you least expect
- Be prepared
- Respond appropriately
- Make sure the right people are engaged
- Communicate, communicate, communicate
MUST HAVES

- Strategy
- Tactical Plans to Respond
- Communication Plan
- Post Breach Activities (Class Action Law Suits, etc.)
ESSENTIALS IN BUILDING A GOOD COMMUNICATION PROTOCOL WITH IT, SECURITY AND LEGAL

- IT/IS, Privacy and Legal must all be tied to the hip
- A Crisis Management Plan must be developed. Create response teams that need to be engaged during the different levels of an event
- Legal plays the most critical role in an enterprise when responding to an event
- Executive leadership needs to buy in to the program if it is to be successful
WHAT DOES IT NEED FROM LEGAL

- Guidance and advice for the CISO and CRO/CCO
- Review and approve response and communications plans
- Work with IT to effectively comply with regulators requests during an event
- Weigh on potential impact to organization
  - e.g., If electronic protected health information (ePHI) is impacted....legal must weigh in on the level of impact to the company - based on the type of data that was breached
Where or how to start?

Building relationships among the key stakeholders

**Step 1: Internal Due Diligence**

*Ask questions and learn everything you can about the data that your company is collecting*

- What are we collecting?
- What is our authorization to collect it?
- Why are we collecting it and how is it being used?
- Is our use consistent with the permission that the data subject has presumably provided when it was first disclosed?
- How does the data move and flow - to where?, from where?
- How long do we retain it?
**Step 2:** Armed with the knowledge obtained from Step 1, explain what data privacy is and why it's important

- **Data Privacy** is the appropriate use of data as determined by cultural norms
  - The EU views data privacy as a fundamental human right whereas in the United States Privacy is often viewed as a consumer protection right.
  - Data Privacy is a matter of cultural respect as much as it is a matter of legal compliance

**Step 3:** Recognize that certain messages will resonate more clearly with different constituencies and tailor your message accordingly

- **Executives, Sales, Marketing** - Data Privacy compliance has a customer impact aspect. It’s a fundamental component of maintaining customer trust and customer intimacy that has both legal consequences and business consequences

- **Information Technology** - Data Privacy compliance has an IT efficiency aspect. It can help the IT Dept. be more efficient by establishing data retention limitations and by facilitating the movement of Personal Data in the EU to servers in the U.S.

- **Insurance & Risk Management** - Data Privacy compliance has an insurance and risk management aspect involving significant new costs and expenses
Communicate the benefits of an Incident Response Plan and an Incident Response Team

- 2016 Ponemon Cost of Data Breach Study - The most important thing a company can do to lower the cost of a data breach is have an IR Plan and an IR Team
  - Second most important thing is use encryption

- EU General Data Protection Regulation 72 hour notification rule - An IR Team will likely increase the probability of compliance with the requirement to notify the applicable EU Supervisory Authority within 72 hours
  - An IR Team following a pre-existing IR Plan will likely reduce confusion, reduce internal conflict and save time

- Federal Acquisition 72 hour notification requirements
  - DFAR 252.204-7012 - Safeguarding of unclassified controlled technology - obligation to report an incident within 72 hours
RECRUIT THE TEAM

A data security incident is a business problem and not just a technical issue
- Senior Executive
- In-House Counsel
- External Counsel
- Information Technology
- Corporate Communications
- Customer Support/Customer Care
- Insurance and Risk Management

Select a Team Leader!
DRAFT AN INCIDENT RESPONSE (IR) PLAN

Create an initial plan. Invite potential IR Team members to the planning sessions

- An Initial IR Plan provides structure and purpose for the IR Team
- Categorize the incidents to which the Plan will apply
- Establish incident severity categories and corresponding levels of deployment

Establish Incident Response team membership that corresponds to different types of Security Incidents

- If a security incident involves employee data - add HR to the team

Establish pre-determined roles, responsibilities and authorizations

- Reduce confusion, internal conflict and save time
LESSONS LEARNED

Insurance & Risk Management are great allies

- Insurance carriers want to see IR Plans and IR Teams in place

Internal Privacy Due Diligence is really important

- Keep probing and asking questions - don’t be surprised when you find new information or information that doesn’t correlate with your previous understanding

Recognize that the development of a Privacy Culture requires constant vigilance and constant internal training

- Employees come and go
- New initiatives are commenced, and new data is collected

Incident response teams need mock drills

- Mock Drills make it real for everyone and help to reinforce the whole idea of a Privacy Compliance culture
QUESTIONS?