About HEMISPHERE Cyber Risk Management, LLC

- Established in 2015
- Professional cyber risk management services
- Proprietary risk modeling
- Specializing in business risk tied to cyber, legal and insurance convergence
Cyber

Business Risk or Just “IT”?
Cyber Risk – What Comes to Mind

Cyber Risk – What “Should” Comes to Mind
2017 National Association of Corporate Directors (NACD) Survey – 14% expressed a deep understanding of cyber risk

All Tied to “Cyber Risk”
Cyber Risk – “That will never happen to me.”

I don’t have time for this “Cyber” stuff! I’m Good! My IT guy told me so.
Fiduciary Duty

“A fiduciary duty is the highest standard of care. The person who has a fiduciary duty is called the fiduciary, and the person to whom he owes the duty, is typically referred to as the principal or the beneficiary. If an individual breaches the fiduciary duties, his or her beneficiaries are entitled to damages, even if they suffered no harm.” ~ Cornell Law 2018

CareFirst Case

SCOTUS held on 2/21/2018 that lower court’s interpretation that “future harm” meets threshold to establish a harm trigger for standing.
Standard of Care vs. Due Diligence

**Audience Questions**

- How many regulations do you comply with today?
- How many risk assessments do you complete a year?
- How much does compliance cost you? (ballpark)
- How many after action reports do you review?
- How do you determine “reasonable” cybersecurity?
- What did you do to remedy the material weaknesses?
What system and data resources are you responsible for?

Data Types to Consider

**Personnel**
- 401
- Social Security Numbers
- Addresses
- DOB
- Personal email
- Telephone numbers
- Fitbit/ health challenges

**Corporate or Business Partner**
- Credit Card/ Banking Information (ACH)
- EHR
- Proprietary data
- Mailing lists
- PII

Your Gateway to Cyber Risk Management
Exposure - Continued

BUSINESS IMPACTS DURING A CYBER EVENT

- Class Actions
- Individual Notification
- Insurance Notification
- Internal Investigation & Forensics
- Business Reputation
- Vendor Involvement & Indemnity
- SEC Disclosures
- Local Law Enforcement FBI
- Breach Response Plan (Call centers/Credit Monitoring)
- Federal Regulator Enforcement (FTC, GDPR, HHS, DFAR)
- State Attorney General
- M&A Valuation
Securities Lawsuits

Litigious shareholders are eyeing fresh opportunities in cyberattacks.

A particular strand of shareholder lawsuits—securities fraud class actions following data breaches on publicly traded companies—are rising in tandem with the frequency of such attacks.

Shareholders have filed nine such class actions since January 2017 under federal securities law, Bloomberg Law data show. None were filed the year before, according to the data. Equifax Inc. and Intel Corp. are among the companies named in those suits, which typically allege that data breaches or system vulnerabilities led to falling stock prices. Two of the suits have been voluntarily dismissed, the rest are ongoing.

These securities-related lawsuits could be more problematic for companies than the shareholder derivative suits more typically seen after cyber breaches. Courts have often dismissed derivative suits—in which a shareholder can sue a company board on behalf of the company for breach of fiduciary duty—due to a high legal hurdle for plaintiffs.
Case Study Number 1 – Equifax

2017

May/June – breach occurs

Sept 7 – Breach made public
Sept 8 – Stock tanks
Sept 12 – Cyber staff “retiring”
Sept 15 – Sr. Cyber Staff “retiring”
Sept 21 – Bogus Website Detected
Sept 26, CEO Forced to retire

19 days
Case Study Number 2 – Uber

Hackers compromise Uber accessing 57 million records

Uber elects to use “hush money”

Uber elects not to apply standard of care and intentionally does not notify 48 state Attorney Generals
NYDFS Cybersecurity and NAIC Model Laws & GDPR

Operational Readiness Discussion
Cross Policy Convergence – When Harm Triggers may Invalidate 3rd Party Policies
Applying Lessons Learned

Breakout Session – Scenario Based
June 6, 2018

You are the CEO of HUBRIS, a $500M a year financial services company operating in New York City, Tokyo, Japan, and Frankfurt, Germany. The company has a Board of Directors and employs 750 people scattered across the U.S., Japan, and Europe. HUBRIS recently underwent an independent audit for Sarbanes Oxley compliance and received a Report of Compliance (ROC) just last month. The I.T. department consists of 30 people with varying degrees of experience and responsibility.
Scenario

The head of your information technology department (CIO) advises you that a corporate issued laptop to an employee in New York was identified as having suspicious activities communicating with an I.P. address in North Korea. To date, HUBRIS’ IT department maintains responsibility for all IT matters, including cybersecurity and a CISO is not employed in any manner.

Upon further review, this laptop had a version of mobile code (Adobe) that was vulnerable to hacking and the IT department had suspended the employee’s account access and the laptop was taken offline to re-image the device and assess the scope of the breach.

As the CEO, what questions or steps should you be taking at this point?
Scenario

June 24th, 2018

HUBRIS General Counsel contacts you over the weekend to advise she was contacted by the FBI about information regarding a hack of HUBRIS. No further details provided and you schedule a meeting with the FBI on the morning of the 26th.

June 26th, 2018

The FBI advises you that all information about to be shared is deemed “law enforcement sensitive” and should not be disseminated outside of those in the room. A Russian organized crime gang known as “GotU” is operating in Crimea and intelligence supports they spoofed North Korean IP addresses to disguise their activities. GotU appears to have successfully infiltrated HUBRIS back on June 1st after an unnamed employee visited a website that was hosting malware on it.
Scenario

The extent of the cyber incident confirms over 250 gigabytes of data were sent outside of HUBRIS’ network. While the data was encrypted the IP addresses tied to the FBI investigation were not limited to the one laptop. Several IP addresses tied to HUBRIS assets were identified as sending data out to the designated North Korean IP address.

After the FBI debrief you, the General Counsel asks about the recent audit they underwent and why it didn’t pick this activity up. The CIO was brought in and upon further discovery, the additional IP addresses belong to Human Resources and Finance Departments.

What should you do next?
What mandatory requirements apply to this event?

What policies and plans exist for HUBRIS for cybersecurity and crisis management?

What legal consequences is HUBRIS exposed to?