

The Rapid Evolution of Cyber Liability

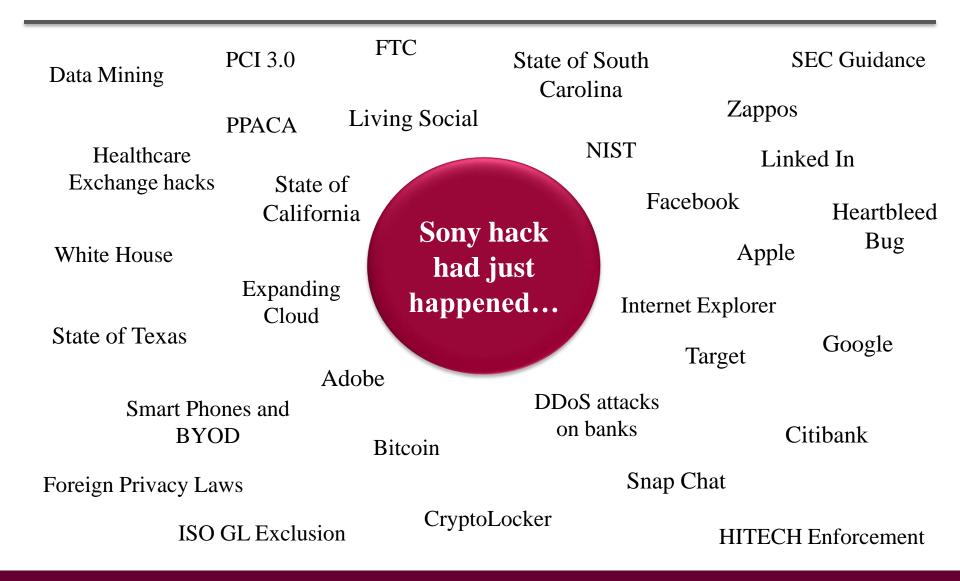
May 29, 2014

University of Connecticut School of Law



- Introductions
- The State of Cyber
 - Claim Trends
 - Insurance Market
- Evolving Cyber Exposures
 - The Cloud
 - Data Security and Internal Procedures
 - BYOD
- Developing Legal Environment
 - Healthcare
 - Payment Card Industry
 - NIST
 - Litigation







The Panel:

- Charles Bellingrath, Product Leader for Privacy, Network Security,
 Technology and Media Liability at ARC Excess & Surplus of New England
- Christopher Novak, Co-Founder and Global Director of the Investigative Response Unit at Verizon
- Robert Wice, U.S. Focus Group Leader for the Technology, Media and Business Services team at Beazley

Moderator:

Jason Glasgow, CyberRisk Product Manager at Travelers



State of the Cyber Market

"I do not think that means what you think it means."

- What do we mean by Cyber?
- What does the market for Cyber look like?
- What coverage is available?



State of the Cyber Market

"I was on a bus that flipped over 17 times."

- Claim trends
 - Retail
 - Healthcare
 - Those two obscuring where the real action is?



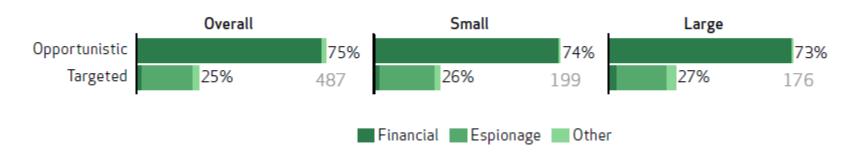
Breach Count by Data Variety & Motive

Financial	376	37	100	47	1		2	7	10	6	1	13
Espionage	1	1	119	1	1	3	1	113	122	119		21
Activism	2		3	8	1			2	4			
Other	1	1	14	6			1	2	10			8
	Payment	Bank	Credentials	Personal	Medical	Classified	Copyrighted	System	Internal	Secrets	Other	Unknown



Attack Targeting

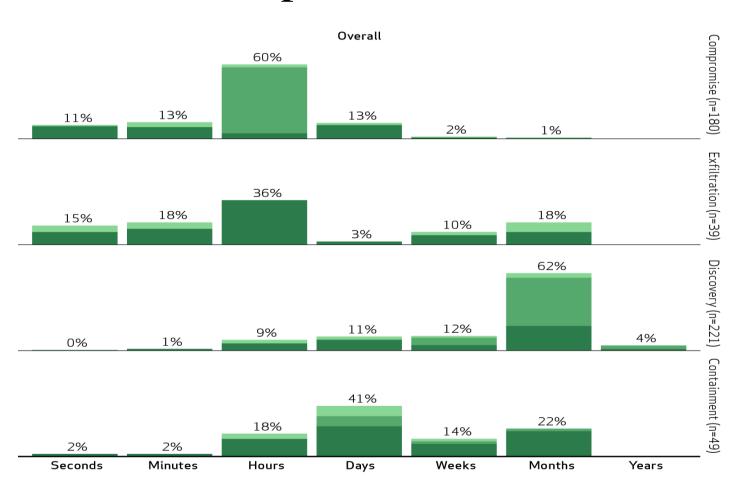
Figure 38: Attack targeting







Timespan of Events





State of the Cyber Market

"Come on, guys! It's all ball bearings these days!"

- Is there an industry that doesn't need Cyber?
- Cyber a standard purchase?
- Coverage overlap?
- CGL changes?





Evolving Exposures

- The Cloud
- Internal Cyber Protocols
- Vendor Selection
- Mobile Devices



Protecting Healthcare Data

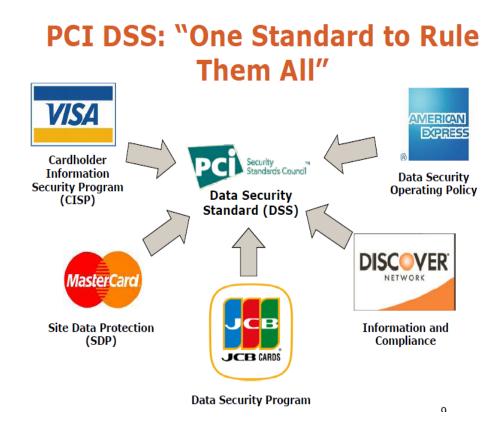
- HIPAA
- HITECH
- HHS Audits
- OCR Enforcement
- Impact of PPACA?





The Payment Card Industry

- Standard that is applied to:
 - Merchants
 - Service Providers (Third Third-party vendor, gateways)
 - Systems (Hardware, software)
- That:
 - Stores cardholder data
 - *Transmits* cardholder data
 - Processes cardholder data
- Applies to:
 - Electronic Transactions
 - Paper Transactions





PCI DSS Overview:

Issuing Bank

Bank that issues payment cards to consumers (cardholders)

Acquiring Bank

Contracts for payment services with merchant; merchant must validate PCI DSS compliance with its "acquirer"; acquirer reports compliance status to card associations

Merchant

Entity that sells goods/services and accepts cards; responsible for safeguarding credit card data and complying with the PCI DSS

Service Provider

Entity that provides all or some of the payment services for the merchant; responsible for safeguarding credit card data and complying with the PCI DSS

Recently released Version 3.0 is more process-based, less point-in-time.

PCI contractual penalties.



Cyber Regulatory Environment, Non-Healthcare Division

- Kentucky joining the club!
- Thanks a lot, Florida!!
- NIST framework for information sharing
- FFEIC guidance
- SEC examination of registered advisors



Cyber Legal Environment

- PCI challenge cases
- Sony case CGL case
- DSW Shoes Crime case

Claims

- What's the typical claim?
- Big guys more info; but are small and mid-size easier targets?