

**Cybersecurity:
Emerging Legal Risks**

Data Breach Cyber Liability Seminar

April 17, 2015

By: Tsutomu L. Johnson
tj@scmlaw.com

- Data Breaches: JP Morgan, Home Depot, P.F. Chang's, Healthcare.gov, and Sony
- The developer for Norton Antivirus revealed that their product works less than 45% of the time
- The average cost of a data breach in the U.S. is more than \$6 million. The average number of records lost is about 30,000 and the cost for each lost record is about \$201 [Source: Ponemon Institute]
- More than a third of attacks target small business, 60% of those businesses go out of business in 6 months [Source: National Cybersecurity Alliance]

- Identify attack vectors
- Define Personal Identifying Information
- Discuss federal and state cybersecurity laws
- Review cybersecurity solutions

Types of Attacks

- Malware: viruses and trojans
 - Example: Cryptolocker
- Hacking: advanced computing to breach systems
- Social: exploiting human nature
 - Most attacks rely on social deception
 - Example: Target
- Misuse: Employees who fail to follow rules
- Smash and Grab: simple theft
- DoS: Concentrated email attacks against a server

- Organized Crime
 - Example: Nordstrom in Florida
- Hacktivists
 - Example: Snowden
- Government Organizations
 - Example: North Korea and Sony
- Employees

- Personal Identifying Information is:
 - A person's names plus:
 - Driver license number, SSN, credit card number, financial account numbers, or passport information
- Organizations collect this information from I-9s, W-2s, credit card machines, direct deposits, and health insurance plans
- Hackers can use this information to file fake tax returns, create fake credit cards, and fraudulently purchase goods online

– HIPAA

- Regulates organizations that collect personal health information: information indicating someone received or sought health care
- Applies to covered entities: doctors, hospitals, health insurance brokers, companies with 50+ full-time employees
- Covered entities must protect the confidentiality, integrity, and availability of personal health information
- Penalties:
 - \$100 to \$10,000 fine for each individual affected, per day, until breach is resolved
 - Continual audits from the Office of Civil Rights

State Regulations

- 48 state statutes regulate personal information
- In Utah, anyone who gathers personal indentifying information must protect that information and take efforts to destroy that information
- If you have a breach, you can't just follow Utah law, you have to apply the law from the states where your customers reside
 - Example: 10,000 document data breach
- Penalties:
 - Wide variety of penalties; in Utah, the fine can be up to \$2,500 for each lost document

- PCI-DSS (Payment Card Industry Data Security Standard)
 - Regulatory scheme from cardbrands like Visa and Mastercard
 - More than 200 points of compliance to securely process credit cards
 - Has a private fee structure for failing to comply with PCI-DSS standards
 - Fees are tiered based on number of transactions; if an organization fails compliance once, the cardbrands place that organization in the highest tier for fees

- Organizations are not required to create an impenetrable defense, but they need to address cybersecurity risk
- Cybersecurity requires three groups of people:
 - IT: They perform vulnerability assessments, identify how to strengthen security, and locate technical solutions to cybersecurity risks
 - Attorneys: This group coordinates the data breach response and develops policies and procedures that comply with the law
 - Insurance: Insurance can be a cost effective way to shift risk.
 - Note: CGL policies do not cover data breaches

- Password Policies
- VPN access for remote devices
- Creating a life-cycle for Assets containing PII
- Train Employees about PII and data security
- Create Bring Your Own Device Policies to regulate information on employee-owned devices
- Encrypt Assets containing PII

- Develop an information security program
- Find cyber insurance
 - Note: CGL policies do not cover data breaches
- Get a risk assessment
- Store information remotely so you can restore lost information
- If you have a breach, call an attorney



SNOW
CHRISTENSEN
MARTINEAU

CYBER DEFENSE LAW GROUP

**For questions or more information please feel
free to contact me directly:**

Tsutomu L. Johnson

tj@scmlaw.com

801-322-9112

Thank you for your time!