MURTHA MEANS
MORE
INDUSTRY INSIGHT

INFORMATION SECURITY AND PRIVACY GROUP NEWS

March 2016

CYBERSECURITY CONFERENCE - ESSENTIAL TAKE-AWAYS
PROTECTING YOUR DIGITAL ASSETS: GOVERNMENT, INDUSTRY AND LEGAL PERSPECTIVES

BY BURT COHEN

Representatives of Connecticut businesses and corporations, educational institutions, and state and local government attended Murtha Cullina's March 2016 Cybersecurity Conference at the Quinnipiac University School of Law. Featured speakers were ***Assistant Attorney General Matthew Fitzsimmons****, who heads up the Department of Privacy and Data Security for the Office of the Connecticut Attorney General;* ***Rob Howley, Senior Director of Regulatory Affairs for Cox Communications****; and* ***David Gardiner, Cyber Intelligence Analyst for the FBI,*** *based in New Haven, Connecticut. In addition, 5 Murtha attorneys provided key tips on privacy and data security risks:* ***Jen Corvo****, on data security in the workplace;* ***Stephanie Sobkowiak****, on healthcare privacy issues;* ***Ryan Suerth****, on business insurance coverage issues;* ***Suzanne Walsh****, on access to digital accounts and assets after an account-holder's incapacity or death; and* ***Ted Whittemore****, on corporate board obligations for data security.* ***Burt Cohen, Chair of Murtha Cullina's Information Security & Privacy Practice Group****, gave introductory remarks and moderated the panel discussions.*

Below are essential take-aways from the conference:

The Problem of Cybersecurity

- **515 data breach notifications affecting 2.5 million Connecticut residents** were made to the Connecticut Attorney General's Office in 2015.
- **Motivations for cyberattacks** can be categorized as follows: (1) to obtain personal and financial information; (2) to obtain financial gain; (3) for revenge or to cause disruption to a business; and (4) as part of a nation-state attack.
- **Data breaches** can occur from an external threat or an internal source, caused by negligence or thoughtlessness, or through a vendor or contractor.
- **Former employees** or a less than honorable employee can also create serious data security issues.
- An **advanced persistent threat (APT)** involves a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. Typically, the intention of an APT attack is to steal data rather than to cause damage to the network or organization. However, most every cyber-attack is persistent in that there is advance reconnaissance and planning that goes into the execution of the breach.

For Questions About Information Security Matters, Please Contact:

Burt Cohen, Chair
bcohen@murthalaw.com

Heather O. Berchem
hberchem@murthalaw.com

Michael P. Connolly
mconnolly@murthalaw.com

Jennifer A. Corvo
jcorvo@murthalaw.com

Rachel Snow Kindseth
rkindseth@murthalaw.com

Bruce L. McDermott
bmcdermott@murthalaw.com

James F. Radke
jradke@murthalaw.com

Stephanie Sprague Sobkowiak
ssobkowiak@murthalaw.com

Ryan M. Suerth
rsuerth@murthalaw.com

David R. Sullivan
drsullivan@murthalaw.com

Suzanne Brown Walsh
swalsh@murthalaw.com

Edward B. Whittemore
ewhittemore@murthalaw.com

MURTHA CULLINA LLP
ATTORNEYS AT LAW MURTHALAW.COM

BOSTON
HARTFORD
NEW HAVEN
STAMFORD
WHITE PLAINS
WOBURN

- **Business email compromises (BEC)** are sophisticated intrusions of legitimate business email accounts that result in simulated, yet bogus, emails that request wire transfers or other sensitive data. During the past year, there was a reported loss of $1 billion dollars due to business email compromise.
- **Utility company scammers** obtain information about a business's account information for electric, water or gas service, and then they proceed to contact by phone or sometimes in person the business usually at a peak operating time and threaten shut-off unless immediate payment is made. Utilities, however, have a clear termination procedure, so any such demand for payment is fraudulent.
- **Phishing** is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), by masquerading as a trustworthy entity in an email.
- **Ransomware** prevents or limits users from accessing their own computer system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back.
- **Tech support scams** can involve computer pop-ups but more commonly telephone calls that purport to be from a legitimate company, such as Microsoft, seeking access to your computer or network claiming to fix computer problems or to enhance computer performance.
- **It is critical to monitor** your own company's or organization's network to ensure that it has not been infiltrated; otherwise, your network could be programmed to attack other networks.
- **The U.S. Department of Homeland Security has identified 16 critical infrastructure sectors in the U.S.:**

Chemical Industry	Dams	Financial Services	Info Technology
Commercial Facilities	Defense Industry	Food & Agriculture	Nuclear Industry
Communications	Emergency Services	Government Facilities	Transportation
Critical Manufacturing	Energy Industry	Healthcare Industry	Water Supply System

Cybersecurity from a Legal Perspective

- Although many businesses and industries are subject to specific federal laws regarding the protection of personal and confidential information and records, there is **no single federal law that applies across the board to data security and breaches.**
- As of now, **47 states have enacted their own laws for handling data breaches**, including CT, MA, RI and NY.
- **An emerging trend** is for a state to enforce its own data security and breach of law on out-of-state companies when a data breach occurs involving the disclosure of personal information on that state's residents.
- **Connecticut law imposes restrictions on the posting, displaying, transmission and use of social security numbers**, including prohibiting any person or business from requiring a social security number over an unencrypted web connection or to access a website without also requiring a password. (Conn. Gen. Stat. § 42-470)
- **Connecticut law mandates that any person who collects social security numbers in the course of business must create a privacy policy** and publish or publicly display it, such as on that business's website. The privacy policy must protect the confidentiality of, limit access to and prohibit the unlawful disclosure of any such social security numbers. (Conn. Gen. Stat. § 42-471)
- **Connecticut law requires persons and businesses to safeguard data**, computer files and documents containing personal information on another person from misuse by third parties and also requires that any such data, computer files and documents must be destroyed, erased or made unreadable prior to disposal. (Conn. Gen. Stat. § 42-471)
- **Connecticut law requires that notification of a breach** of personal information must be provided to affected persons and the Office of the Attorney General within 90 days from discovery, when that personal information has not been secured by encryption or any other technology that renders the information unreadable or unusable. Personal information means the first name or initial and last name in combination with one or more of the following: (1) social security number; (2) driver's license number; or (3) account number, credit or debit card number, in combination with a security code, access or passcode. (Conn. Gen. Stat. § 36a-701b)

- In addition to enforcing these statutes, the **Connecticut Attorney General can also enforce certain privacy-related federal laws**, such as HIPAA which protects individually identifiable health information, whether in written or electronic format. The Connecticut Attorney General was the first state AG to sue a breaching party under HIPAA. In the health care industry, HIPAA is arguably broader than the Connecticut law, although a breach under HIPAA is often a data breach under Connecticut law, as well.
- **A business that makes untrue representations about its privacy and data security may be subject to a lawsuit** under the Connecticut Unfair Trade Practices Act or an enforcement action by the Federal Trade Commission.
- **Corporate boards have a legal duty of oversight for cybersecurity** and, as part of that duty of oversight, should regularly consider and oversee management's efforts to address data and information security issues as a material business risk.

Best Practices to Address Cyber Risks

- **It is essential to have a written information security program (WISP)** that not only provides a working guide on how to react in the event of a data breach or a cyber-attack, but also involves an internal self-examination of your practices to protect and secure confidential information on your employees, customers, clients and patients.
- **Each company and organization should also focus on the human element through Cybersecurity training** and periodic testing of personnel to ensure that proper safeguards and established computer protocols are being followed.
- **Cyber liability/crime insurance** is now offered to cover a variety of both liability and property losses from conducting business on the Internet or collecting data within its internal electronic network. These policies cover a busines's liability for a data breach in which customers' personal information is exposed or stolen by a hacker or other criminal who has gained access to the firm's computer network. The policies typically cover a variety of expenses associated with data breaches, including: notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft. They may also cover Ransomware situations. Before purchasing any such insurance, consider having the policy reviewed by an insurance attorney or professional.
- **Corporate boards should ask questions of management** concerning data security and breaches. It may make sense to appoint a board member who is conversant in data security issues or hire outside security experts to review corporate preparedness for cybersecurity threats.
- **Utilize encryption** both in the storage of electronic data but also in any transmission or distribution of electronic data, particularly when it involves personal and confidential information.

And now for something completely different . . .

- **Modern estate plans must address access to digital accounts and assets** after an account holder's incapacity or death. Otherwise, in many cases, federal privacy laws will prohibit fiduciary access altogether, regardless of the asset's values.
- **Digital or electronic currency will undoubtedly become more common over time.** The goal is to establish uniform laws and standards that minimize the opportunity to utilize these currencies for illegal money laundering. Murtha attorney Suzanne Walsh serves on the Uniform Law Commission's Drafting Committee on the Regulation of Virtual Currency Businesses which is drafting model regulations for this nascent industry.
- Counterintuitively, **bitcoins, the most recognizable digital currency, cannot be easily used for money laundering, according to the FBI,** as the transactions are publicly traceable.

According to the Identity Theft Resource Center there were a total of 110 data breaches and almost 1.8 million records exposed during just the first two months of 2016. Moving forward we can expect the volume of data breaches to continue to increase. This means that the challenges of protecting individuals, businesses and organizations from new threats, as well as staying compliant with new laws and regulations, will become much more complex.

If you have any questions regarding information security issues, please contact:
Burt Cohen at (203) 772-7714 or bcohen@murthalaw.com