ALSTON&BIRD

LEGAL ISSUES IN SHARING CYBER THREAT INTELLIGENCE: WHAT ARE THE REAL CONCERNS?

Kim Peretti

September 9, 2015

2015 Cybersecurity Innovation Forum

Agenda

- The Cyber Threat Landscape
- The Legal Justification for Information Sharing
- A Closer Look at What Data is Shared
- What Are the Legal Concerns (And Are They Real)?
- A Comparison to Proposed Legislation
- Guidance for Establishing Information Sharing Programs

The Cyber Threat Landscape

ABC NEWS

CareFirst Says Data Breach Affects About 1.1M People

CNBC

Report of credit card breach at Mandarin Oriental

Sign Up at irs.gov Before Crooks Do It For You

National Security, Cyber Espionage, and Bulk PII Breaches

THE WALL STREET JOURNAL.

Health Insurer Anthem Hit by Hackers

Breach Gets Away With Names, Social Security Numbers of Customers, Employees

PREMERA | BLUE CROSS

Premera has been the target of a sophisticated cyberattack

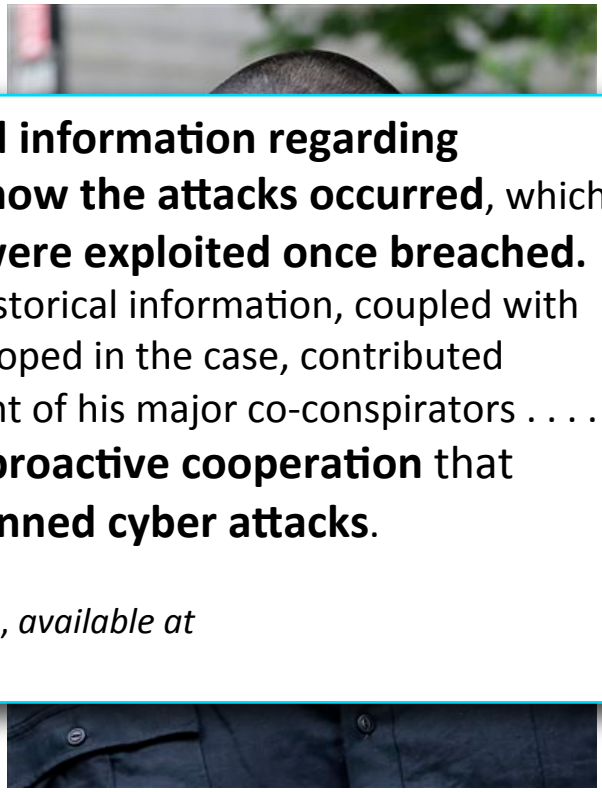
The Washington Post

Hacks of OPM databases compromised 22.1 million people, federal authorities say

Information is Key to Cyber Defense

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of NEW YORK

HECTOR MONSEGUR, a/k/a "Sabu," formerly a leading member of a group of sophisticated computer hackers known as "LulzSec," was sentenced today in Manhattan federal court to time served and one year of supervised release for his participation in computer hacking activity that victimized media outlets, government agencies and contractors, and private corporations around the world by hacking into, disabling, and at times exfiltrating data from the victims' computer systems. MONSEGUR pled guilty in August 2011 to computer hacking conspiracy, computer hacking, computer hacking in furtherance of fraud, conspiracy to commit access device fraud, conspiracy to commit bank fraud, and aggravated identity theft pursuant to a cooperation agreement with the Government. U.S. District Judge Loretta A. Preska imposed today's sentence.



Monsegur subsequently and timely provided **crucial, detailed information regarding computer intrusions** committed by these groups, including **how the attacks occurred**, which members were involved, and **how the computer systems were exploited once breached.** As set forth below, Monsegur's consistent and corroborated historical information, coupled with his substantial proactive cooperation and other evidence developed in the case, contributed directly to the identification, prosecution and conviction of eight of his major co-conspirators . . . . On top of that, Monsegur engaged in additional, **substantial proactive cooperation** that **enabled the FBI to prevent a substantial number of planned cyber attacks**.

United States v. Monsegur, No. 11 CR. 666 (LAP) (S.D.N.Y. May 23, 2014), *available at* http://www.wired.com/wp-content/uploads/2014/05/Monsegur.pdf.

Information Sharing – A Legal Justification

Information Sharing Overview

A "critical aspect of next generation information security is the ability to share and receive actionable threat intelligence in a timely manner . . . . By working together with government to disseminate and receive cyber threat information, companies can learn where to look for signs of an attack and how to alter their security systems to 'plug holes' and block attempted intrusions carried out using techniques that were effective in earlier attacks."

- Tom Litchford, VP of Retail Technology, National Retail Federation

Testimony before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime* (Apr. 16, 2014).

Fast Access to Threat Data

REUTERS EDITION: U.S.

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

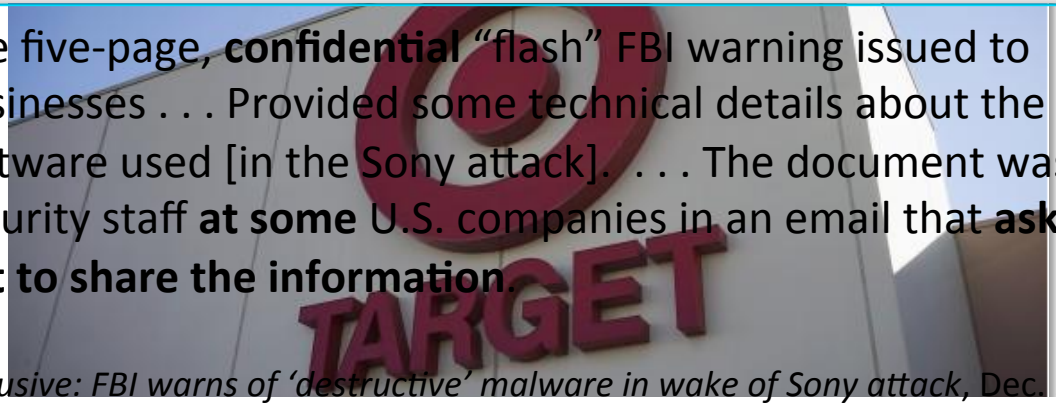
Tue Dec 2, 2014 2:56am EST

Related: TECH, ARTS, CYBERSECURIT

Exclusive: FBI warns of 'destructive' malware in wake of Sony attack

BOSTON | BY JIM FINKLE

The five-page, **confidential** "flash" FBI warning issued to businesses . . . Provided some technical details about the malicious software used [in the Sony attack]. . . . The document was sent to security staff **at some** U.S. companies in an email that **asked them not to share the information**.



(Reuters) - The FBI has warned U.S. retailers to prepare for more cyber attacks after discovering about 20 hacking cases in the past year that involved the same kind of malicious software used against Target Corp in the holiday shopping season.

Exclusive: FBI warns of 'destructive' malware in wake of Sony attack, Dec. 2, 2014, Jim Finkle and Mark Hosenball, *Reuters available at* http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202

By the Numbers. . .

- **82%** Percentage of "High Performing" Information Security companies that "collaborate with others to deepen their knowledge of security and threat trends."
- **61%** Percentage of IT Security Professionals who believe that "exchanging threat intelligence . . . Could have prevented their organization from experiencing a cyberattack in the past 24 months."
- **$451,000** – Average estimated monetary loss from each security incident

Source: PricewaterhouseCoopers LLP, U.S. Cybercrime: Rising risks, reduced readiness 2014 (June 2014), available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/ publications/assets/ 2014-us-state-of-cybercrime.pdf

Benefits of Information Sharing

1. Prevent/Defend Cyberattacks: Early receipt of critical threat data is key

2. Security Standards Alone Insufficient: Compliance-based strategies are insufficient in the face of sophisticated, evolving cyber threat actors

3. Fight Fire with Fire: Criminals collaborate and share information to carry out cybercrime we should do the same

Regulator Expectations

FFIEC Cybersecurity Assessment General Observations

During the summer of 2014, Federal Financial Institutions Examination Council (FFIEC)

"Many financial institutions rely on media reports and third-party service providers to gather information on cyber events and vulnerabilities. Financial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerabilities so they may evaluate risk and respond accordingly. **Participating in information sharing forums (e.g., Financial Services Information Sharing and Analysis Center) is an important element of a financial institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents.**"

financial institution's cybersecurity inherent risk incorporates the type, volume, and complexity of operational considerations, such as connection types, products and services offered, and technologies used.

Connection Types

Questions to Consider

- What types of connections does my financial institution have?

Information Sharing Models/Networks

- Private Sector
  - Peer-to-peer sharing
  - Informal group discussions
  - Post-to-All or Listserv Model
  - ISACs/ISAOs
- Public Sector
  - NCCIC – National Cybersecurity & Communications Integration Center
  - NCIJTF – National Cyber Investigative Joint Task Force
  - CISCP – Critical Infrastructure Cyber Information Sharing and Collaboration Program
  - IC3 - Internet Crime Complaint Center

What Data is Shared?

Actionable Threat Intelligence

What Actionable Threat Intelligence IS:

- Technical Data – Information that an IT security team can use to prevent, detect or block an attack
  - Name of malware and its hash values
  - IP addresses used in prior attacks

- Tactics, Techniques and Procedures – the "TTPs" cybercriminals use to exploit systems:
  - Tactic: Using malware to steal credit card information
  - Technique: Sending an e-mail embedded with keystroke logging malware to capture credit card data
  - Procedure: Registering a domain to create legitimate-looking e-mail accounts that will circumvent antivirus protections and spam blockers

Actionable Threat Intelligence

What Actionable Threat Intelligence is NOT (or does not need to be):

- Personally Identifiable Information ("PII")
  - Names, credit card data and other sensitive information are not threat intelligence
- Trade Secrets
  - Sensitive internal corporate information is often the ***target*** of cyber attacks, not the data shared to prevent them

What Are the Legal Concerns? (And Are They Real?)

Four Common Concerns

1. Antitrust Concerns
2. Future Disclosure Through FOIA Requests
3. Violations of Legal Obligations Related to Privacy Protections
4. Lack of Protection from Regulatory Action or Civil Liability

Antitrust Concerns

The Concern:

- Sharing information on cyber threats could be interpreted by government regulators as "anti-competitive behavior"
- In recent study, 26% of IT professionals identified antitrust concerns as one of their three top reasons for not sharing threat information
- **Says the CPO**: If I share threat data, my company is going to face unwanted scrutiny from DOJ Antitrust

Antitrust Concerns (cont'd)

- DOJ/FTC Policy Statement on Information Sharing and Antitrust: In April, 2014 the agencies tried to allay these concerns:
  - Real issue for agencies was sharing of competitively sensitive information such as "current, and future prices, cost data, or output levels" that allow for "competitive coordination among competitors"
  - Engaging in information-sharing mechanisms were deemed "not likely to raise antitrust concerns"

FOIA Requests

The Concern:

- Data provided to the government will be discoverable through FOIA requests

- **Says the CPO**: Engaging in information sharing will make my company's private, proprietary information discoverable by the public, and our competitors

FOIA Requests (cont'd)

- Limited Scope: FOIA only applies to data shared with the government.
- Proposed Legislation: Every recently proposed legislative initiative on information sharing has included FOIA protections (*See* CISPA, SECURE IT Act and the Cybersecurity Act of 2012)
- Currently, only Limited Data is Protected: The Protected Critical Infrastructure Information (PCII) Program protects certain data from disclosure through FOIA and state, tribal and local laws. But it has limitations:
  - Applies only to data related to critical infrastructure entities
  - May not apply to all actionable threat intelligence
  - Data is only protected if shared with DHS through the PCII Program
- Consider existing FOIA protections: E.g., many state laws exempt confidential, proprietary and/or trade secret data from disclosure

Violations of Privacy Protections

The Concern:

- State and federal privacy laws and contractual obligations govern the collection, storage, use and disclosure of personal, sensitive or otherwise regulated data
- **Says the CPO**: If I engage in information sharing, I'm putting my company at risk of enforcement actions, civil lawsuits, and breach of contract for violating privacy laws and other obligations.

Violations of Privacy (cont'd)

- Actionable Threat Intelligence is generally <u>not</u> privacy-related information or can be stripped of such information without losing its essential value
- **<u>DOJ White Paper on SCA</u>: The Stored Communication Act ("SCA") prohibits communications service providers (like ISPs) from disclosing customer information to outside parties**
  - **In May, 2014, the DOJ released a paper stating that communications companies can share "non-content information to the government" in its "aggregate form" meaning it cannot be connected to a single customer**

No Liability Limitations

The Concern:

- There are no safe harbor or liability protections related to information shared either among the private sector or with the government

- **Says the CPO**: We've just had a breach and if I share actionable threat intelligence with the government, the regulators are going to use that knowledge to bring an enforcement action against my company for failing to implement reasonable data security practices or comply with other obligations

No Liability Limitations

- Government Enforcement Actions:
  - Under what circumstances could information shared with the government be shared with another branch/ department/agency?
  - Under what circumstances would regulators request information shared with information sharing forums or otherwise come across that information?
- Bolstering Civil Class Actions:
  - Under what circumstances would information shared with the government discoverable through FOIA requests by class action plaintiffs? Or information shared with ISAOs through discovery/subpoena requests?

A Comparison to Proposed Legislation

Proposed Legislation

- Protecting Cyber Networks Act (PCNA) (H.R. 1560)
  - Passed the House in April, 2015 (H.R. 1560)
- Cybersecurity Information Sharing Act (CISA) (S. 754)
  - Introduced (but not passed) in the Senate in 2014 and 2015
- Both Include Significant Liability/Disclosure Protections:
  - Antitrust Exemptions: Generally exempts private entities from antitrust laws for sharing cyber threat intelligence
  - Civil Liability Protections: Liability protections granted except in cases of gross negligence or willful misconduct
  - Enforcement Action Protections: Shared threat indicators and defensive measures may **not** be used to regulate the "lawful activities" of private entities
  - FOIA/State Law Disclosure Protections: Shared information is expressly granted FOIA protection **as well as** protection from disclosure under state laws
  - Removal of PII: Requires that private entities and the federal government remove PII from all shared threat data

Guidance for Safe Information Sharing

Guidance for Sharing Information

- Understand Your Current Sharing Efforts:
  - Many IT security professionals share data on an informal basis
  - Have your legal department review current sharing efforts and identify potential risks

- Establish Written Procedures for Information Sharing:
  - Who? What? When? With Whom? How?
  - Establish protocols when there may be a significant incident and/or data breach
    - Ensure legal is aware/involved
  - Ensure information sharing is part of the company's incident response protocols

Guidance for Sharing Information

- Protect Privileged Data:
  - A key benefit of engaging outside counsel is conducting a privileged investigation
  - Sharing threat intelligence is unlikely to break that privilege, but tread carefully
- Understand Protections in Data Requests:
  - Law Enforcement Investigations: Responses to grand jury subpoenas are protected by substantial secrecy laws
    - Consider requesting that government entities seek cyber threat data using subpoena powers
    - Ask for advance notice before law enforcement shares threat intel with broader government community

Private Sector Information Sharing

- Understand Protections (cont'd)
  - DHS Requests: Data shared with DHS through the PCII Program is protected
    - Consider leveraging that program when possible
- Have a Share-First Mentality
  - Trust ISACs/ISAOs and established Listservs
- Share Smart
  - Use anonymity measures and redact data when possible

Guidance for Sharing Information

- Ask for Protections:
  - When regulators ask for threat intel, request FOIA exemptions
  - Many state laws exempt confidential, proprietary and/or trade secret data from disclosure
- Discuss Options for Regulator Requests (As Needed):
  - Obama administration has illustrated a clear goal of creating a robust information-sharing environment
  - After a data breach (or otherwise) if regulators request data provided in information sharing efforts, engage in dialogue to discuss options.

Bottom Line(s)

- The Good: Information Sharing is a crucial tool in the fight against cybercrime that companies should leverage as much as possible

- The Bad: Additional liability and FOIA protections are still needed to create a robust information sharing environment

About Alston & Bird's Privacy and Data Security Practice:

Privacy & Data Security Team

Our team helps clients at every step of the information life cycle, from developing and implementing corporate policies and procedures to representation on transactional matters, public policy and legislative issues, and litigation.

www.alston.com/privacy

Cybersecurity Preparedness and Response Team

Alston & Bird's Cybersecurity Preparedness & Response Team specializes in assisting clients in both preventing and responding to security incidents and data breaches, including all varieties of network intrusion and data loss events.

www.alstonsecurity.com