Sharing Cybersecurity Threat Info With the Government -- Should You Be Afraid To Do So?

Bruce Heiman
K&L Gates

September 10, 2015

Bruce.Heiman@klgates.com
(202) 661-3935

Why share information?

- **Prevention**
  - Timely exposure of threats & vulnerability
  - USG uniquely able to provide threat information/foreign intelligence
  - Facilitates effective cooperation on best way to prevent, detect, address potential harm
- **Protection**
  - USG can distribute information more broadly
  - USG can help mitigate damage
- **Prosecution**
  - USG better positioned to investigate, arrest, pursue cybercriminals domestically and internationally

Why not share information?

- Premature escalation
- Lose control of investigation/response
- Invite further attacks
- Reputational harm
- Regulatory enforcement (criminal/civil)
- State Attorneys General actions
- Civil suits (class actions) by those whose data is compromised
- Shareholder suits
- Congressional investigations
- International enforcement

Sources of legal requirements

Federal:

- FTC
- SEC
- GLBA
- FCRA/FACTA
- HIPAA
- COPPA
- UCC
- FAR

State

- Data breach/cybersecurity laws (47)
- UDAP

Common Law

- Negligence
- Breach of contract

International

- EU (Privacy Regulation)
- Nation states

Types of allegations

- **Failure to do what you say**
  - Deceptive practice
  - Intentional/negligent misrepresentation
- **Failure to say what you should**
  - Failure to (timely) disclose material facts
- **Failure to do what you should**
  - Failure to take reasonable security measures (unfair)
  - Negligence
  - Breach of fiduciary duty/duty of care
  - Breach of contract
- **Failure to disclose a problem**
  - Failure to timely notify of data breach
  - Failure to adequately explain the data breach

So --

How to realize benefits of information sharing and avoid negative consequences?

Answer: **Provide protection to companies to incentivize the voluntary sharing of information among private parties and with the government**.

Current pending legislation

- House:
  - Protecting Cyber Networks Act [HR 1560]
  - National Cybersecurity Protection Advancement Act [HR 1731]
- Senate:
  - Cybersecurity Information Sharing Act (CISA) [S. 754]

Five Key Questions

- Share what kind of information?
- Need to scrub personal information?
- With which USG departments (and who will they share it with)?
- What can the information be used for?
- What legal liability protection will I have?

Share what kind of information?

- "Cyber threat indicator or defensive measure"
- Malware used by malicious actors to compromise computer networks
- Measures to defend an entity's own information networks and system (and those of customers if authorized)

Need to scrub personal information?

- Yes need to:
  - Assess and remove any known personal information identifying a specific person not directly related to a cybersecurity threat or
  - Implement and utilize a technological capability configured to remove such personal information

Share with which USG departments (and who will they share it with)?

- Idea is to create a central portal – DHS and formal process
- Information then rapidly dispersed
- Key issue allegedly is whether information is thereafter shared with DoD and NSA
- A business regulated by a federal agency may share information with that agency and receive protection
- Companies may share information informally with any agency and receive protection [Senate]

How may the information be used?

- Cybersecurity purposes!
- But also: to prevent to respond to the imminent threat of serious national harm, harm to a minor, fraud and identity theft, espionage and trade secrets (Senate – House broader)
- Not to regulate, including by way of enforcement actions, lawful activities
- Important! Those sharing information with the government may impose restrictions on it to use.

What legal liability protections will I have?

- No cause of action for monitoring, sharing or receiving cybersecurity threat information (and acting, or in good faith not acting, on it)
- No waiver of any privilege or protection (including trade secret protection)
- No antitrust violation from sharing information (but cannot fix prices, monopolize etc.)
- Exempt from disclosure under federal or state or local FOIA laws
- Exempt from disclosure under any ex parte requirements
- No limitation on otherwise applicable statutory defenses
- But assumes good faith and reasonable actions
- Does not protect against gross negligence or willful misconduct

Hot topic – defensive measures

- For the first time, pending legislation authorizes "defensive measures" but does not extend legal protection
- Intent: measures to defend one's own networks and systems (and those of customers if authorized by them)
- Not intended to authorize "offensive" measures such as unauthorized access to, or executing computer code on, another entity's information systems
- But recognize that actions on one's own system can have effects on another's system
- Ok unless would *substantially harm* another entity's system

QUESTIONS?

Bruce Heiman
K&L Gates

Bruce.Heiman@klgates.com
(202) 661-3935