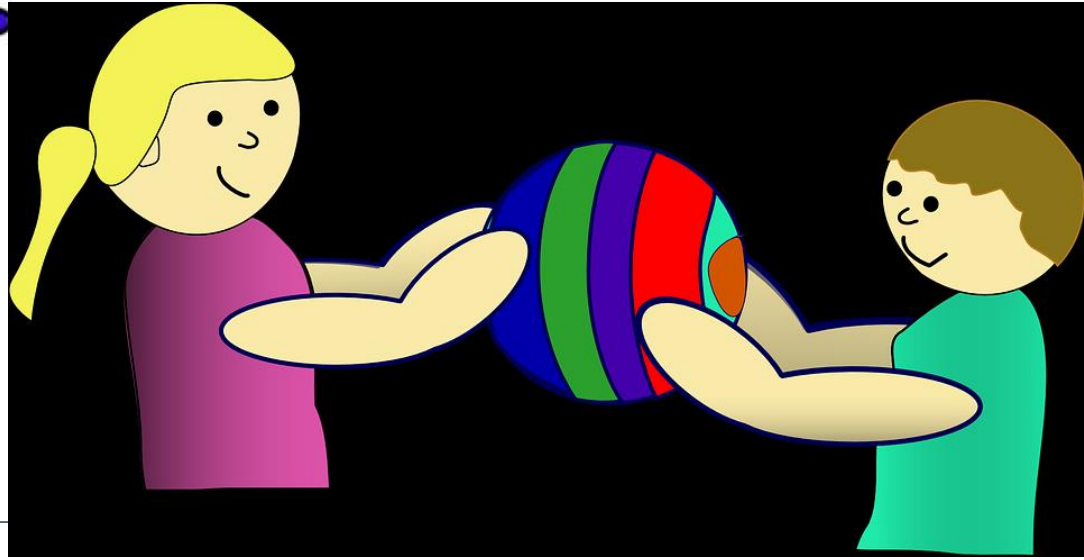

# 2018 SANS CTI Summit

## Legal Implications of Threat Intelligence Sharing

# Law Talking

- Who am I?
  - Former Litigator
  - Chief Privacy Officer
  - Leader of a Cybersecurity Business
  - World-class paranoiac




Department of Homeland Security
Sharing is nice...
Private Companies

# Sharing Your Way to Liability

- Three ways you can be punished for sharing:
  - Sharing too much and too broadly
  - Failing to act on information shared with you
  - Neglecting other security priorities due to burdens of sharing

# BLUF

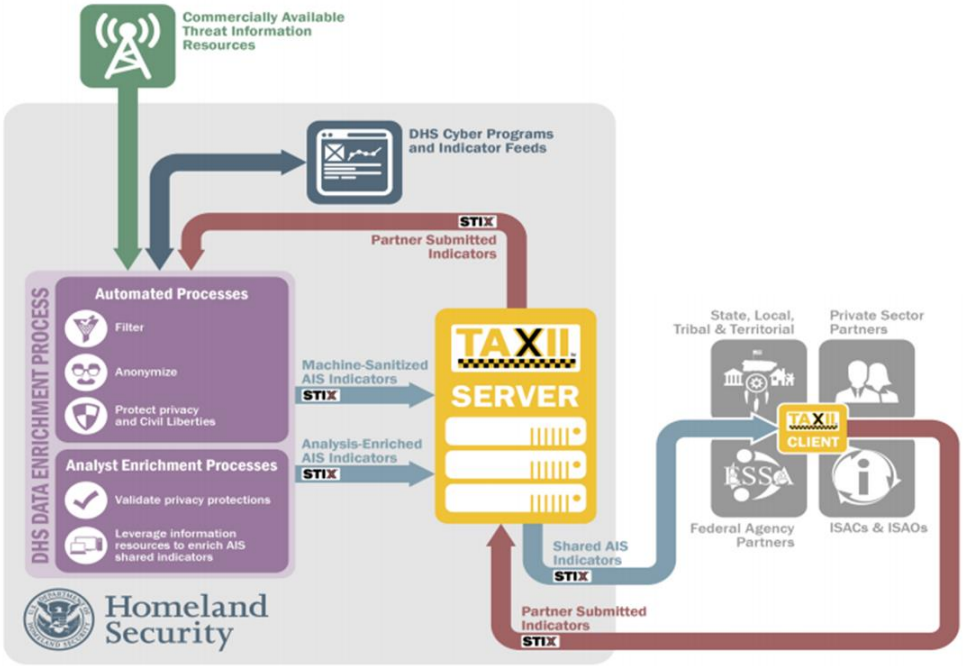
- Threat intelligence sharing can be a critical component of any security program . . . BUT
  - Think before you share - You may inadvertently be CREATING risks for your company by engaging in threat intelligence sharing
  - You must have a plan for how you intend to consume and orchestrate threat intelligence BEFORE you begin receiving external indicators at scale
  - The most valuable threat intelligence originates from your own environment – and stays there.

# What is CISA?


. . . . or just a colossal waste of time and money

# What does CISA do?

- First piece of cybersecurity legislation congress was able to actually pass
- Creates voluntary “peer pressure” system to encourage and facilitate public/private sharing
- Provides liability protection – sort of
- Requires you to remove personal information from indicators



# What does CISA do?

***"Give me your threat intel"***

***"I mean, you know, only if you feel like it."***

***"And we'll totally protect it and PROBABLY won't share it with other agencies."***

***"And if there is stuff in there that makes you look bad, <u>WE</u> won't use it against you – but someone else might."***

# What does CISA NOT do?

- Protect you from liability if you fail to share intelligence the “right” way
- Protect you in the event of a data breach
- Protect you against legal action outside the US

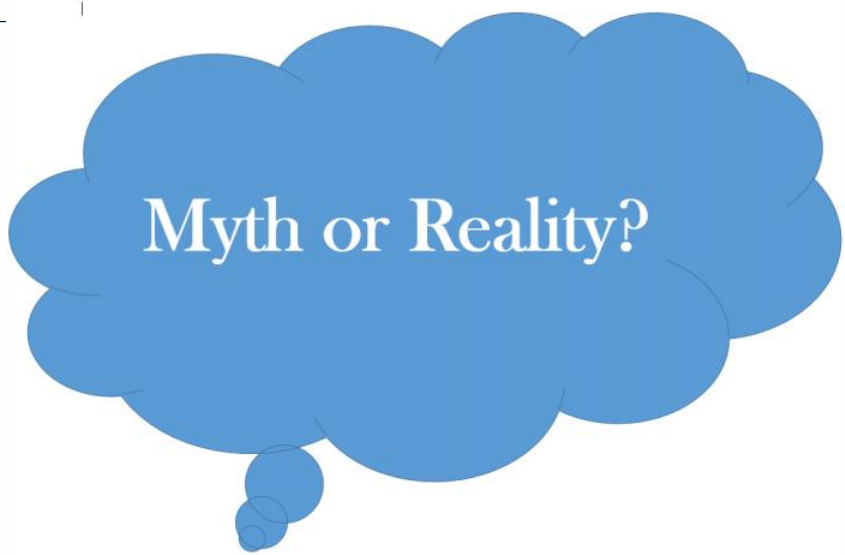
# What does CISA NOT do?

- Cannot Protect Against Legal Actions
  - Negligence
  - Shareholder suits
  - Privacy law violations
  - FTC actions
- No protection for intel you share more casually


You need to recalibrate your risk meter and rethink your assumptions about sharing . . . .

# Myth or Reality

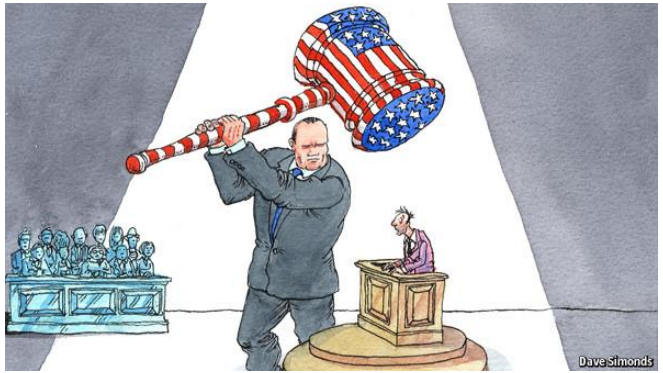
- It can’t hurt if we just receive threat intelligence . . . . right?
- Better to know about a threat then not know
- Can’t possibly stay on top of emerging threats alone, need help and collaboration
- It is a good idea to seek a second opinion from a trusted friend when I find something I think might be bad.



# DISCOVERABLE

# What Every Regulator and Plaintiff Wants to Know (and is NOT afraid to ask) When you Have a Breach

- How did it happen?
- When did you know?
- How did you respond?
- What was exposed (and how do you know)?
- Were you on notice of the risk and what measures were in place to prevent breach?
- What people, process and technology failures contributed to the breach?



Demand is hereby made for the following documents:

1. Documents sufficient to show LabMD's PCI DSS merchant level and SDP merchant level, including any change in merchant level.

2. All data security assessments provided to the Company or any third party related to LabMD, including the following: any PCI DSS or SDP Self-Assessment Questionnaires; assessments by Qualified Security Assessors; Attestations of Compliance with PCI DSS or SDP; or any Reports on Compliance.

3. All communications between or among the Company, LabMD, or any third party regarding LabMD's compliance with PCI DSS and SDP.

4. All external vulnerability scans provided to the Company related to LabMD.

5. Documents sufficient to show all Qualified Security Assessors and Approved Scanning Vendors that have relationships with LabMD, including for each the point of contact, address, telephone number, email address, and facsimile number.

6. All communications between or among the Company, LabMD, or any third party about any security incident at any point in time.

7. All forensic reports or analyses relating to any security incident.

8. Documents sufficient to show all acquiring banks that have a relationship with LabMD, including for each the point of contact, address, telephone number, email address, and facsimile number.

October 24, 2013 By: Megan Cox

# Scenario 1

- Your crack infosec team notices unusual communication to an unknown (but not blacklisted) IP at 3am.
- You investigate and find what appears to be an exfiltration folder on your network.
- You isolate the host immediately, prevent exfiltration, ban processes across your environment and add the IP to your firewall blacklist.
- You confirm that only one host was affected and that no data was exfiltrated.

# Scenario 1

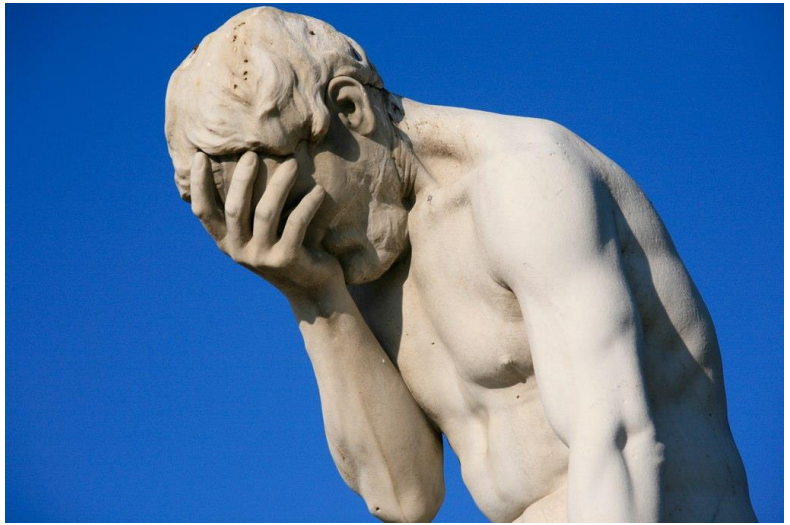
- Your crack infosec team notices unusual communication to an unknown (but not blacklisted) IP at 3am.
- You investigate and find what appears to be an exfiltration folder on your network.
- You isolate the host immediately, prevent exfiltration, ban processes across your environment and add the IP to your firewall blacklist.
- You confirm that only one host was affected and that no data was exfiltrated.
- You proudly share indicators with your ISAO

# Scenario 2

- You consume the indicators you sent to your ISAO after Scenario 1 and ingest them into your SIEM.
- Due to a defective device feed, your correlation rules fail to detect the existence of the same indicator and are exposed (but don’t realize it).
- Four months later, a system administrator notices what appears to be an exfiltration directory on a server.
- Investigation shows that 100GB of TAR files were exfiltrated over preceding months.

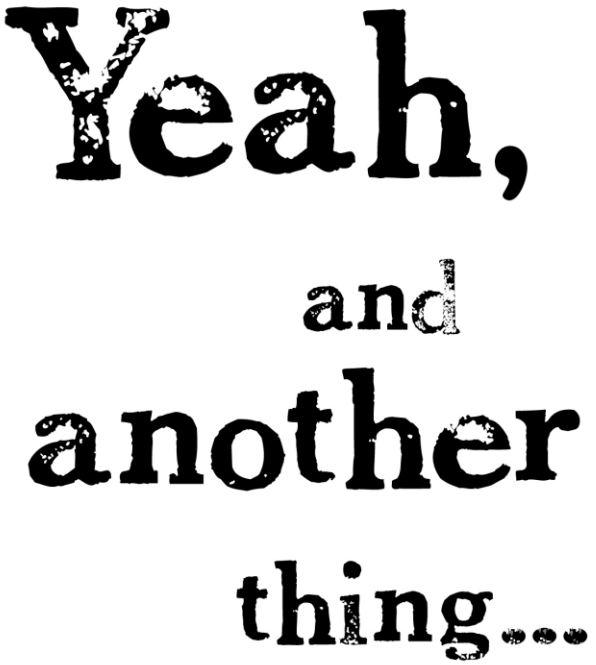
# Scenario 2 (Continued)

- Among information exfiltrated is personal information for 100,000 people
- You notify affected individuals as required in addition to state regulators and issue a “statement” on the breach.
- Someone on the internet connects the dots and realizes that the indicators necessary to detect and prevent the breach were shared via your ISAO 4 months prior.
- When pressed by a regulator, you reveal that you were the one to share the indicators in the first place – and you failed to prevent a second attack.



# How Else Can Sharing Make You LESS SECURE?

- Limited resources to invest in security
- Priorities must start with basic hygeine and critical security controls
- Wasting time chasing false alarms or threats that will never actually materialize for you can detract from higher-impact initiatives
- Signal-to-noise ratio can lead to erosion of trust in threat intel sources



# Take-Aways

- Proceed with caution
- Make sure you have a mature program before you invest much in information sharing
- Don’t give in to peer pressure – or to the desire to validate with peers
- Examine the potential risks for your organization (talk to your attorneys)
- Assume and evaluate the worst possible outcome and act accordingly (practice your Congressional testimony)

# THANK YOU!

**R Jason Straight**

**SVP, Cyber Risk Solutions/CPO**

**UnitedLex Corp.**

**jason.straight@unitedlex.com**