John Wunder, The MITRE Corporation

Challenges and Opportunities in Cyber Information Sharing

Cyber Innovation Forum

September 9, 2015

MITRE

Who am I?

- **I work for MITRE supporting cyber information sharing and cyber situation awareness**

- **MITRE has done this before:**
  - Heavily involved in many sharing communities
  - Support our government sponsors across a variety of capability levels
  - Supported SCAP, STIX™, TAXII™, and others

STIX and TAXII are trademarks of the U.S. Department of Homeland Security

MITRE

What I won't be talking about

Measuring and demonstrating value

Building trust

Hiring talented analysts

Legal issues

MITRE

Challenge 1: You don't know what to share

"What type of cyber information should I be sharing?"

MITRE

Challenge 0: You don't know *why* to share

Information sharing is huge! *But what do we get out of it?*

Understanding **why** to share helps you decide **what** to share.

MITRE

Lesson 0: Why to share

Information sharing is a means to an end

- Identify the problems that **you** need solved and then figure out if more information would help
- There's no one-size-fits-all answer
- Draw up a list of your top ten problems: can any be helped by new information?
- Sharing is a two way street: do you have anything useful for others?

MITRE

Lesson 1: What to share

Once you understand **why** to share and what **problems** it solves, you can understand **what** to share:

Problem / Use Case	Information that can help
Trouble prioritizing resources	Attribution, TTPs
Analysts need more information	Sightings, TTPs
Slow response to major vulnerabilities	Indicators, COA
Lots of spear phishing	Indicators, best practices
Many, many more	

MITRE

Challenge 2: You don't know who to share with

- **There are a lot of sharing groups, commercial providers, etc.**
  - Do you need to join an ISAC? Also, what is an ISAO?
  - Should you join a commercial platform? Which one? Will it be compatible with your tooling and information requirements?
    - Defer this to tooling
- **What do you base the decision(s) on?**
  - Relative maturity? Is more mature always better?
- **You want to receive targeted, relevant intel**
  - How do you identify that?

MITRE

Lesson 2: Who to share with

Once you understand **what** to share, you can identify **who** you can get it from.

Regional

Sector-specific

Commercial platform

Government

Information	Who to get it from
Attribution	Sector, government, commercial
Sightings	Sector, regional, commercial
Best practices	Regional, government

Lesson 2.5: Who to share with

Sharing is a two way street: what do you have that other people can use?

Your data is more valuable than you think!

- **Been doing this two years?**
  - Longer than some.
- **Only taking in indicators?**
  - Sightings are useful!
- **Have advanced capabilities?**
  - Why are you here?
  - Also, your data is obviously valuable ☺

MITRE

Challenge 3: You don't know what tools to use

- It's hard to know what types of tools you need, or how to use them when you get them

- Let alone how to get them integrated

- Do you need a cyber intel repository?

MITRE

Lesson 3: What tools to use

The ones you already have

- **Sharing is not the most important thing your tool does**
  - Pester your tool vendors to support sharing
- **Or, tools to leverage the new information**
  - Just started getting malware samples? Maybe you need an analysis platform?
- **Consider a specialized sharing platform**
  - Do you have a lot of varied incoming information?
  - Do you have a lot of tools that need to be plugged in to that info?

MITRE

Challenge 4: You don't know what to do with STIX and TAXII

- You keep hearing about it, but what does it do for you?
  - As a user do you need to worry about it?

- Or, you know what it does but don't know **which tools** do STIX/TAXII
  - Checkbox compliance still an issue
  - Incompatibilities between popular tools

MITRE

Lesson 4: What to do with STIX and TAXII

Don’t worry about it

- **STIX/TAXII is a means to a means to an end**
- **Tools are continually adding and improving support**

MITRE

Challenge 5: You have trouble sharing in multiple communities

- It's hard to determine what you can re-share and what is either sensitive or copyrighted
- What do you share w/ one group vs. another?
- How do you handle untrusted data?
- Nobody knows what TLP:AMBER means
  - And a lot of people don't know what TLP means
    - (TLP means Traffic Light Protocol)

MITRE

Lesson 5: Sharing across communities

Everyone is still figuring it out

- **There are several coordinated efforts**
  - FIRST working group
  - STIX/TAXII in OASIS
- **Very interested? Participate!**
  - Or at least send in requirements
- **Do the best you can**
  - Understand TLP

MITRE

Challenge 6: You don't know how to provide feedback

- **As a consumer…**
  - What do you do with bad data?
  - What if a producer is repeatedly sending poor quality?
  - Do you have mechanisms to send feedback?

- **As a producer…**
  - Is it worth your time to continue creating content?
  - Are there any actions you can take to improve content?
  - Are you getting anything back from your sharing efforts?

MITRE

Lesson 6: Providing feedback

- **As with all things, start small:**
  - Many sharing platforms are supporting it natively
  - Don't undersell the value of a phone call or e-mail
- **Don't be shy**
- **Building it in: STIX/TAXII are trying to address it**
  - Participate, or submit requirements

MITRE

Challenge 7: You have no idea how to get started

- This is an intimidating space
- There are a lot of moving parts
- No clear guidance forward

MITRE

Lesson 7: How to get started

- **Start small and talk to someone**
  - Solve one problem at a time rather than all at once
  - This is exactly what regional sharing groups are for
- **Not everyone's maturity model ends in the same place**
  - It's OK to not have advanced malware analysis capabilities
  - Look at return on investment
- **Recognize that everyone is growing**
  - Even the more advanced organizations have issues
  - We can all learn from each other

MITRE

Case Study

Your company has recently been hit with a string of spear phishing e-mails targeted at your sector.

Why to share	**Reduce/prevent phishing as a malware vector**
What to share	**Best practices (in)**: how do others prevent phishing? **Indicators (in)**: are there campaigns you can just block? **Sightings (out):** help others analyze data / trends
Who to share with	**Sector-based groups:** For indicators, to share sightings **Regional groups:** For best practices **Government:** Indicators, best practices

MITRE

Case Study (2)

Goal: Reduce/prevent phishing as a malware vector

What tools to use	**Spam gateways:** Indicator ingest **Education tools:** User training **Indicator repository:** Management across sharing groups
STIX/TAXII	**Spam gateway:** Indicator ingest, sightings egest **Indicator repository:** Indicators and sightings, context
Feedback	**Feedback on indicators:** Sightings, corrections **Feedback on practices:** Your own best practices

MITRE

Questions?

John Wunder
jwunder@mitre.org

MITRE