CTI Information Sharing

Active supporters' contributions

- *Andras Iklody*
- *Bret Jordan*
- *Raymond van der Velde*
- *Trey Darley*

Facilitators*:* *Jane Ginn, Stavros Lingris*

Cyber-Threat Information

- ***Cyber-threat information*** is any information that can help an organization to **identify**, **assess**, **monitor**, and **respond** to cyber-threats. Examples of cyber-threat information include indicators (system artifacts or observables associated with an attack), TTPs, security alerts, threat intelligence reports, and recommended security tool configurations.

NIST SP 800-150

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Cyber Threat Intelligence Subtypes

https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf

Cyber Information Sharing

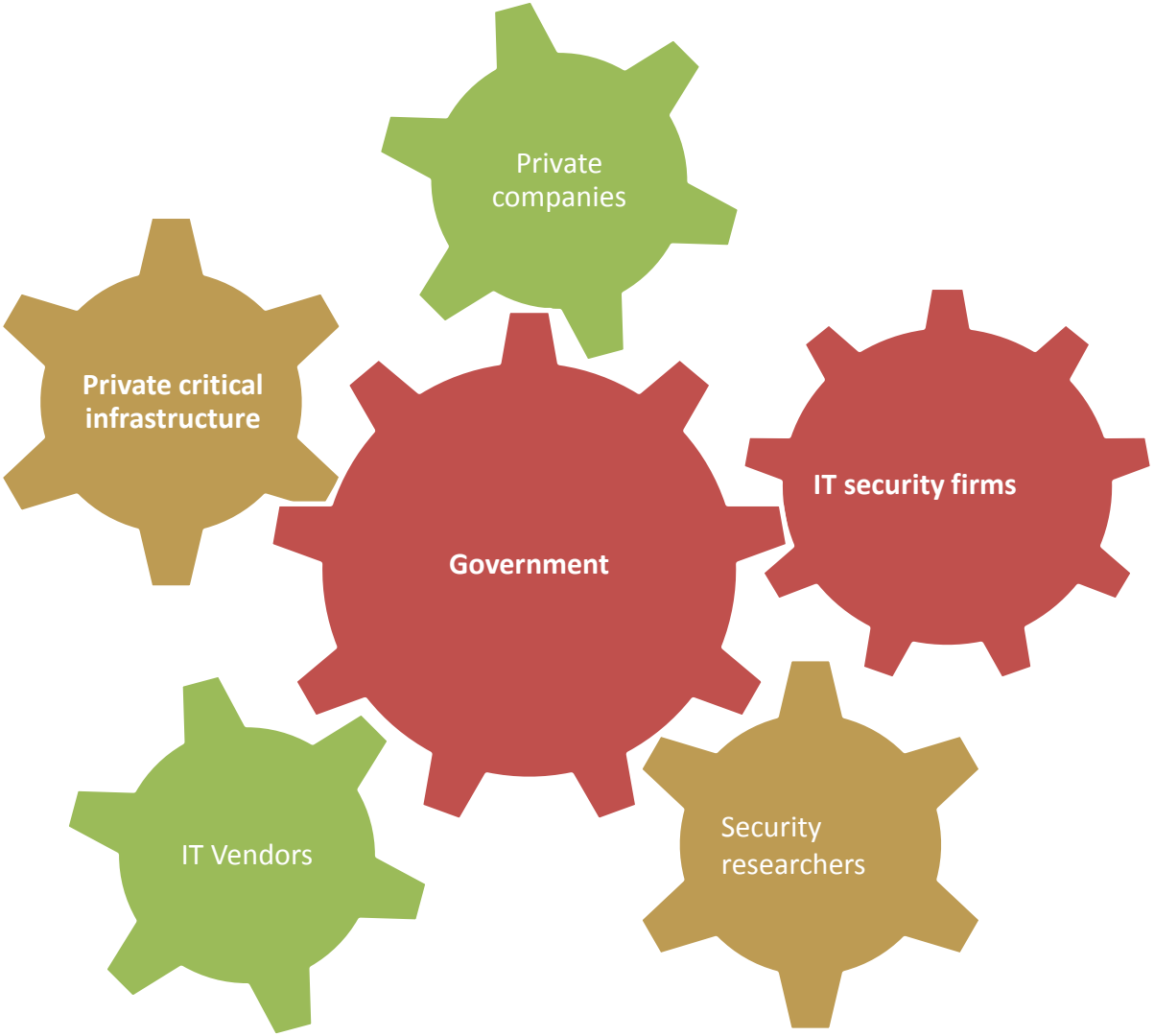
- Information sharing means ‘the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice’

(Robinson & Disley, 2010).
https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

CTI Sharing Driving Factors

- **Legal and Regulatory Drivers for Sharing CTI**
  - US –EO - Improving Critical Infrastructure Cybersecurity
  - EU - **N**etwork and **I**nformation **S**ecurity (**NIS**) Directive
  - Canadian Cyber Threat Exchange
  - EU – GDPR **G**eneral **D**ata **P**rotection **R**egulation
- **Economic drivers**
  - Empower decision-makers to reduce risks
  - Reduce remediation cost from Data Breaches

Information Sharing Actors



Standards for Formatting CTI Information

CTI Information Sharing Initiatives

Europe	US
Abusehelper (https://github.com/abusesa/abusehelper, Community add-ons https://bitbucket.org/ahcommunity/)	Collective Intelligence Framework (http://csirtgadgets.org/collective-intelligence-framework/)
EclectIQ (https://www.eclecticiq.com/)	CRITS (https://crits.github.io/)
IntelMQ (https://github.com/certtools/intelmq)	Soltra (https://www.soltra.com/en/)
Megatron (https://github.com/cert-se/megatron-java)	
MISP (https://github.com/MISP/MISP)	
N6 – CERT.PL	
Warden (https://warden.cesnet.cz//en/index)	

CTI Information Sharing Barries

Operational Barriers

- Lack of trust between participants
- Unavailability of knowledgeable, experienced employees

Technical Barriers

- Lack of common standards
- Large variety of Taxonomies and used protocols
- Additional technical resources required

Financial Barriers

- Additional costs for infrastructure, data feeds and human resources.
- No direct return of investment

Legal/Policy issues

- Lack of General Security agreement
- Information sharing depends highly on local / legal requirements.

Common questions related to Information Sharing

- Who should share information with?
- Is it relevant, adequate, accurate and delivered on time?
- Is delivered via secure channels?
- What Information sharing mechanisms are going to be used?
- Are shared information able to be consumed by all parties?
- How shared information can be used?

“one organization’s detection to become another’s prevention”