What You Don’t Know Can Harm You

Merike Kaeo, CTO
merike@fsi.io
DISCUSSION POINTS

• Introduction and Background
• Barriers to Sharing
• Communities of Trust
• Global Efforts To Bring About Action
• Evolving Standards and Frameworks
• Being Part of the Solution
• Work History
  – IID (*CISO*, 2013-2014)
  – Farsight Security (*CTO*, 2014 – present)

• Industry Recognition/Participation
  – Authored “Designing Network Security”
  – Active Contributor to IETF Standards
  – SSAC member (ICANN)
  – IP6 Forum fellow since 2007
  – Member of FCC CSRIC III (Botnet remediation)
  – Member of EU NIS WG2
BARRIERS TO SHARING

**Technical**
Creating the resilient infrastructure for data sharing that can support a variety of data types and formats.

**Policy**
Creating the appropriate legal structure(s) to foster comprehensive data sharing without cumbersome legal liabilities.

**Governance**
Business rules by which members of a network share, what they share, and with whom they share.
A PERIOD OF RAPID CHANGE

• Intelligent, interconnected devices are continuing to be connected to the global Internet
• Data is accumulating faster than it can be organized or effectively protected
• The complexity of the Internet ecosystem creates a rich environment exploitable by activists, criminals, and nation states
• Data will continue be stolen or modified using subtle, persistent, directed attacks
CRIMINALS HAVE NO BARRIERS

- Websites advertise Botnets and malware for hire
- Vulnerabilities and Exploits are traded on open market
- There are no enforced rules for NOT sharing
- Social media is making sharing more efficient

Choose Custom Botnet
- Number of Hosts
- Geographic Region
- Bandwidth
- Duration
- etc
BREAKING THE BARRIERS OF SHARING

- Legal
- Technical
  - Interoperability
  - End to end automation
- Procedural
- Trust Issues
- Insufficient Interest
COMMUNITIES OF TRUST

IETF  ENISA  ICANN  BlackHat  Defcon
ITU  NIST  ISOC  RSA  MAAWG  Secret Squirrel
APNIC  AfriNIC  RIPE  ISOI  Confluence
ARIN  LacNIC  Underground Economy
APWG  DCC  *-ISAC  MACCSA  FIRST
Secure  SchmooCon  StopBadware  ACD C
AND THERE’S MORE…

• Industry Sectors

• National Initiatives
  UN, NATO, EU, Africa, National CERTs, etc.
GLOBAL EFFORTS FOR ACTION

• **DNS-OARC:** DNS System Security
• **FIRST:** Vulnerability management
• **ISACs:** Specialized Interest Groups
• **M3AAWG / APWG:** Anti SPAM, Phishing and Crime
• **NSP-SEC:** Big Backbone Providers and IP Based Remediation
• **OPSEC-Trust:** Situational Awareness
MODELS, METHODS AND MECHANISMS

• Models of Exchange
  – Voluntary exchange vs Mandatory disclosure

• Methods of Exchange
  – Trust-based
  – Formalized
  – Security clearance-based
  – Ad-hoc

• Mechanisms of Exchange
  – Person to person
  – Machine to machine
THE UNKNOWN – HOW CAN IT HARM YOU?

- Estonia Example (2007)
  - Creating **trust**
    - TC-FIRST
    - Global Operation Security Teams
  - Cross functional meetings
  - Known roles due to e-voting (2005)
  - Government **facilitated** communication and tactics
  - Openness with **information sharing** was critical
DO YOU HAVE A CIRT?

• You Should Have a Computer Incident response Team
  – Who is part of this?
  – What are their responsibilities?

• Important – Define a single individual to be in charge (also have a backup for that individual)

• Know who you need to contact
  – Legal / regulatory responsibility
  – Upstream ISPs who may help filter on DDoS attacks
  – Impacted individuals
CONTINUE TO INCREASE SHARING

• Initial Step – Build Trust Thru Networking

• Start by sharing for specific use cases that don’t impact privacy and personally identifiable information (PII)
  – SSH Brute Force Attacks
  – DNS/SMTP/NTP Amplification Attacks
  – Passive DNS Information

• Investigate how to share data that may impact privacy/PII and what can be anonymized but still be useful
  – SPAM / Phishing details
THOUGHTS ON PASSIVE DNS

- DNS is used by ALL electronic communications
- pDNS still new to many people despite existing since 2004
- PII issues depend on where you do your observations
- Valuable data that is shared to get information on malware campaigns
EVOLVING STANDARDS & FRAMEWORKS

• FIRST Initiatives
  – Traffic Light Protocol (TLP) SIG
  – Information Exchange Policy (IEP) SIG
  – Information Sharing SIG

• OASIS
  – Cybox/STIX/TAXII

• Other Ongoing Work
  – NIST / ENISA
  – IETF
## TLP – OLD VS EVOLVING

<table>
<thead>
<tr>
<th>Color</th>
<th>When should it be used?</th>
<th>How may it be shared?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</td>
<td>Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</td>
<td>Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</td>
<td>Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.</td>
</tr>
<tr>
<td><strong>WHITE</strong></td>
<td>Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</td>
<td>TLP: WHITE information may be distributed without restriction, subject to copyright controls.</td>
</tr>
</tbody>
</table>
WHAT CREATES POLICY COMPLEXITY?

• Variations in global privacy laws and legal liability
  – Many sharing initiatives based on bi-lateral agreements

• Variations in policy interpretations
  – Who do you share with?
  – How do you protect data?
  – What are you allowed to do with the data?
INFORMATION EXCHANGE POLICY (IEP)

• Work started over 2 years ago

• FIRST was natural place to get global participation

• Initial v1.0 Framework done
  – https://www.first.org/global/sigs/iep
  – Information Sharing SIG utilizing it
  – Unifying with OASIS STIX

• Work ongoing
  – Other operational sharing groups asking for clarifications
**IEP SPECIFICS**

**Information Exchange Policy Framework**

**Handling**
- Defines how to protect information e.g. encrypt at rest
- Handling supports Sharing and Action

**Action**
- Defines permitted uses of information e.g. passive actions, externally visible actions, disruption
- Value comes from actionable information
- Complex due to business models

**Sharing**
- Defines permitted redistribution of information e.g. the Traffic Light Protocol (WHITE, GREEN, AMBER, RED)

**Licensing**
- Defines the license or terms of use for information
- May include references to applicable policies, partnership agreements or sharing agreements
IEP and STIX

- **IEP Appendix A**
  - STIX JSON representation of an IEP implementation

- **Close collaboration with OASIS**
  - STIX 2.0 documentation has reference to IEP
  - IEP work ongoing to include IEP within STIX
BEING PART OF THE SOLUTION

• Participate in policy work
• Work with national CIRT teams
• Help formulate privacy laws that protect citizens personal privacy but don’t hinder protecting critical electronic communications
• Share what you can and help cross-functional education
QUESTIONS ?