Microsoft Security Response Alliance
SUMMIT

Microsoft

Automating Information Exchange
- *The Policy Factor*

Merike Kaeo, CEO, Double Shot Security
Paul McKitrick, Senior Security Strategist, MSRC
Steve Mancini, Threat Intelligence Strategist, Intel

Session Agenda

Information Exchange 101

Ecosystem Trends

Information Exchange Challenges

The Policy Factor!

Information Exchange Policy Framework Straw-man

Join the discussion!

Who am I? Paul McKitrick

Passionate about Security Automation and Information Exchange

Senior Security Strategist, Microsoft Security Response Center

Worked for government, non profits, and the private sector:

- Technical security operations
- Coordinating national level incident response
- Stakeholder engagement and information sharing programs
- Security policy – developed the .nz DNSSEC policy
- Founder of the New Zealand Internet Task Force www.nzitf.org.nz

Who am I? Merike Kaeo

Work History

- National Institute of Health (1988-1993)
- Cisco (1993-2000)
- IID (2013-2015)
- Double Shot Security (2000-present)

Industry Recognition

- Authored "Designing Network Security" by Cisco Press (1999 / 2003)
- Active Contributor to Multiple IETF Standards
- Trusted Member in Many Informal Information Exchange Forums
- Member of SSAC (Security Stability Advisory Council for ICANN) since 2010
- Member of FCC CSRIC III (Botnet Remediation) and FCC CSRIC IV (DNS/Routing)

Who am I? Steve Mancini

my $DAYJOB = “Intel Corporation”;

- IT Threat Intelligence Strategist
- Team Lead, Advanced Adversary Response Team
- Program Manager, Emerging Threat Analysis

Industry Mayhem:

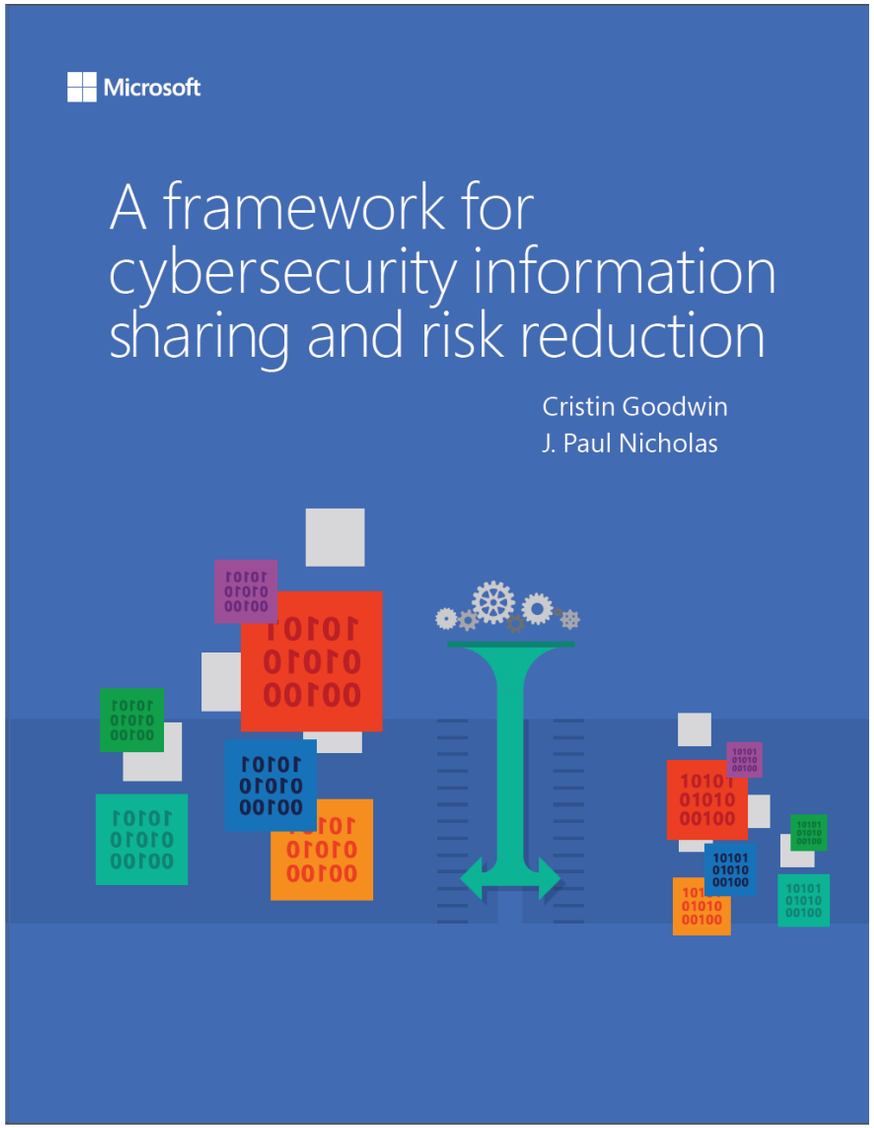
- Author RAPIER, open source client triage tool
- Threat Information Sharing partnerships / trust circles
- AudioParasitics Security Podcast Member
- Defcon CTF veteran

"With more than **one million cybersecurity positions unfilled worldwide**, currently-identified security needs couldn't be met if every employee at GM, Costco, Home Depot, Delta, and Procter & Gamble became security experts tomorrow."

- Leviathan Security Group 2015

Information Exchange 101

Information Sharing Whitepaper



http://aka.ms/infosharing

- Types of Cybersecurity Information
- Models of exchange
- Methods of exchange
- Mechanisms of exchange
- Information formats
- Actors Involved
- Sharing Communities

Cybersecurity Information and formats

Information types

- Best Practices
- Incidents
- Mitigations
- Situational Awareness
- Strategic Analysis
- Threats
- Vulnerabilities

Information formats

- Human readable
  - Emails, documents, reports etc
- Machine Readable
  - Semi structured e.g. flat text files, .tsv, .csv
  - Highly structured e.g. STIX, IODEF, OpenIOC

Exchange Models, Methods and Mechanisms

Models of exchange

- Voluntary exchange models
- Mandatory disclosure models

Mechanisms of exchange

- Person to person
- Machine to machine

Methods of exchange

- Trust-based
- Formalized
- Security clearance-based
- Ad hoc

Sharing Actors and Communities

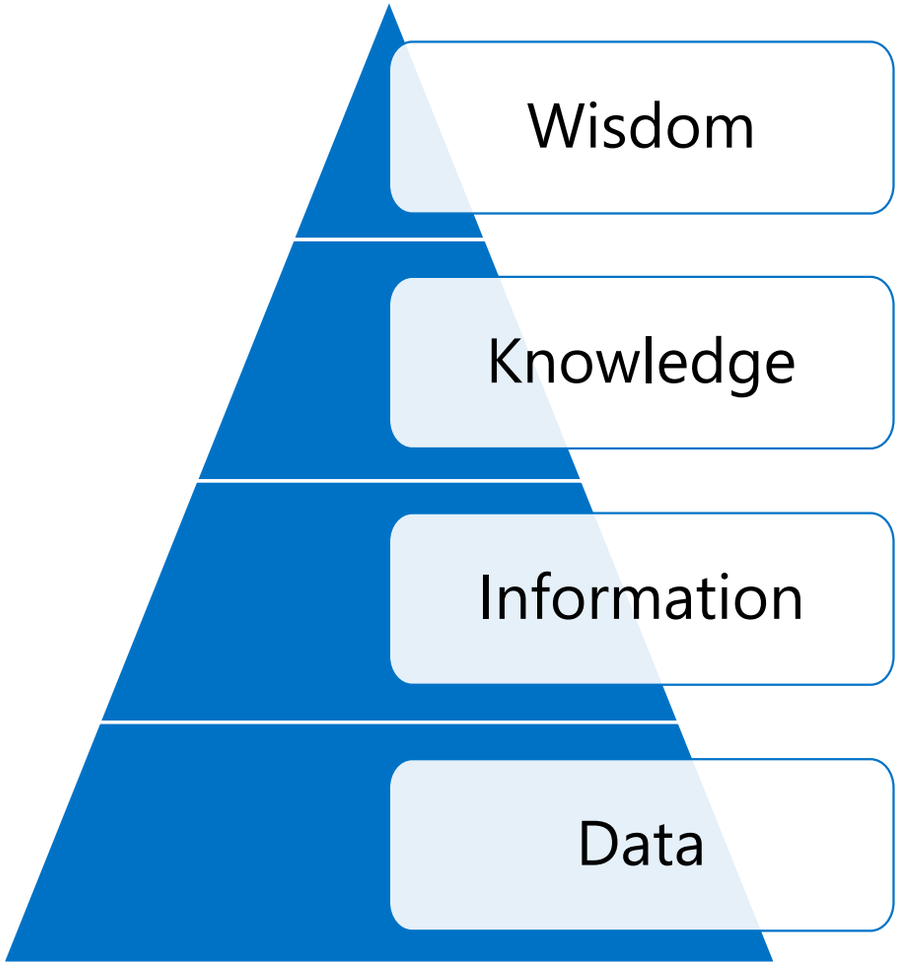
Sharing Actors

- Government
- Private critical infrastructure
- Business enterprises
- IT Companies
- IT security firms
- Security Researchers

Sharing Communities

- Trust based
- Geographical scope
- Operational scope
- Common interests
- Common concerns
- Sector specific

Data Information Knowledge Wisdom (DIKW)



Situational Awareness is intelligence across a range of areas / threats

Intelligence about specific areas / threats / groups / families

Contextualized and curated event logs

Atomic facts and raw event logs

Reference: https://www.farsightsecurity.com/Blog/20150701-bapril-dikw/

Security Intelligence 101

Security Intelligence encompasses Operational Intelligence, Threat Intelligence, and Vulnerability Intelligence

Each category has different characteristics and suitability for automation

Security Intelligence 101

Security Intelligence encompasses Operational Intelligence, Threat Intelligence, and Vulnerability Intelligence

Each category has different characteristics and suitability for automation

Aligns with Law Enforcement aspects of crime

- Means e.g. technical skills
- Motive e.g. motivation ☺
- Opportunity e.g. new/existing vulnerability

Characteristics of Operational Intelligence

Supports reactive Incident Response

Traditional abuse and fraud reporting e.g.

- Email accounts or servers sending spam
- IP Addresses DDoSing and Scanning
- Compromised websites

Machine generated and readable information

Generally more concrete, discrete, consistent information that is well suited for automation

'Digital exhaust' that is often 'dropped on the floor'

Characteristics of Threat Intelligence

Supports proactive and reactive Incident Response

Provides context to threats, actors, and groups

Human generated / readable reports and descriptions

Generally more abstract, disparate and variable information that is not well suited for automation

Processing of machine readable indicators can be more easily automated, but requires scenario / context for automated responses

Characteristics of Vulnerability Intelligence

Supports proactive and reactive Incident Response

Details about new vulnerabilities and affected systems

Internal tracking of systems and their software versions

Tracking dependencies and versions of code and libraries

Telemetry / sightings of attempted use

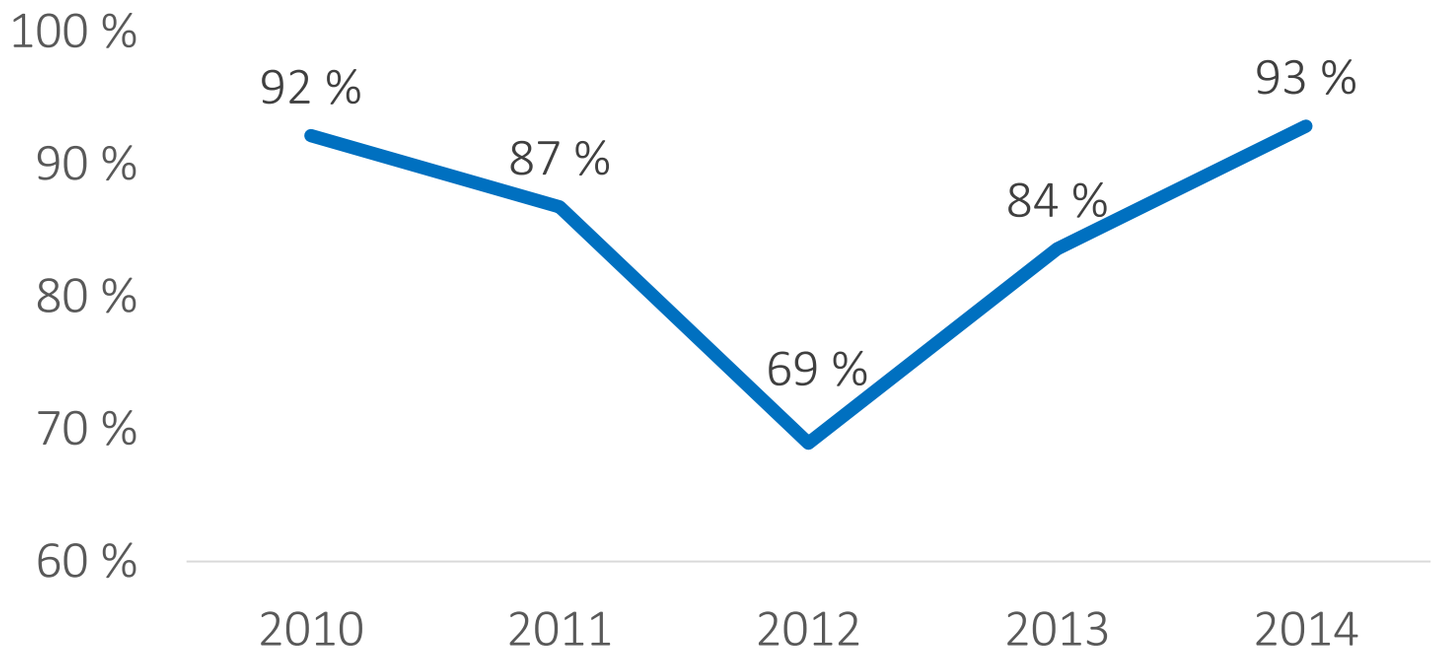
Information is suited for automation

Ecosystem Trends

Ecosystem Trends

Breaches discovered through third party notifications

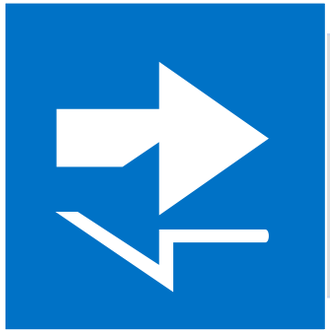
93%



Source: Verizon 2015 Data Breach Investigation Report

Information Sharing Trends

'Assume Breach' driving demand for intelligence



'Give-to-get' mindset gaining popularity

Organizations increasingly willing to share

Industry Trends

‘Threat intelligence’ is a valuable commodity

Rapidly growing volumes of ‘threat intelligence’

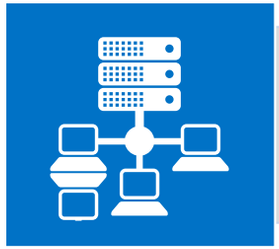
Organizations are ill prepared to automate

Information Exchange Challenges

Organizational Challenges

Skill set shortages

Lack of end to end automation



Limited interoperability

Inadequate policy

What about the Traffic Light Protocol (TLP)?

Color	When should it be used?	How may it be shared?
RED	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.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	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.	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.
GREEN	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.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	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.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Source: https://www.us-cert.gov/tlp

The Policy Factor!

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"

-Bruce Schneier

Why is policy necessary?

Organizations need appropriate agreements and governing rules for approval to automate information exchanges in order to:

- Limit an organizations liability and risk from exchanging information
- Manage risk for staff involved in exchanging information
- Ensure partner expectations are met and information is used appropriately
- Protect valuable sources of information from inadvertent mistakes

The policy and governance aspects of automating information exchange are as complex as the technical challenges

What creates policy complexity?

Who you share with and what you are allowed to share depends on the use case (abuse desk vs remediation vs investigation, etc)

- How do you protect data that has been shared with you?
- What are you allowed to do with data that is shared?

Variations in global privacy laws and legal liability

- Todays sharing initiatives are based on multitudes of bilateral agreements

Cohesiveness and collaboration is needed between technologists, governmental policy advisors and legal experts

Typical conversation with legal council

Hi, we would like to share some information with our security partners

What do you want to share? Who do you want to share with?

Lists of IP addresses scanning or attacking our network, with all of the MSRA partners!

Hmm, dodgy crowd that MSRA lot…

What are they going to do with it?

Who are they going to share it with?

How will you control that? …

The overall policy goals?

Cohesiveness and consolidation to avoid future need to support and translate a multitude of policy frameworks

Improve the ability to convey and interpret policy associated with exchanging security and threat information

Information Exchange Policy Framework Straw-man

A straw-man proposal is a brainstormed simple draft proposal intended to generate discussion of its disadvantages and to provoke the generation of new and better proposals.

Source: Wikipedia ‘Straw-man Proposal’

Straw-man Guiding Principles

1. Don’t reinvent the wheel
2. Keep it Simple
3. Keep it Extensible
4. Internationally Applicable
5. Technology Agnostic
6. Interoperable with other frameworks / taxonomies

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

Information Exchange Policy Framework Straw-man

Handling

ENCRYPT IN TRANSIT (MUST | OPTIONAL)

ENCRYPT AT REST (MUST | OPTIONAL)

Action

NO ACTION e.g. TLP RED

INTERNALLY VISIBLE ACTIONS e.g. Internal scanning and correlation

EXTERNALLY VISIBLE PASSIVE ACTIONS e.g. DNS Lookups

EXTERNALLY VISIBLE ACTIVE ACTIONS e.g. botnet takedowns

Information Exchange Policy Framework Straw-man

Sharing

REDISTRIBUTION

- **NONE**
- **INTERNAL**
- **EXTERNAL VICTIM NOTIFICATIONS** e.g. data only pertaining to a victim
- **EXTERNAL TRUSTED PARTNERS** e.g. trusted industry partners and communities
- **PUBLICALLY RELEASEABLE**

SOURCE ATTRIBUTION (Producer or Publisher)

- **ATTRIBUTE** (MUST | MUST NOT | OPTIONAL)

OBFUSCATION (Victim or Attacker)

- **OBFUSACTE SOURCE** (MUST | OPTIONAL)
- **OBFUSACTE DESTINATION** (MUST | OPTIONAL)

Information Exchange Policy Framework Straw-man

Licensing

COMMERCIAL USE

NOTIFICATION SERVICES (YES | NO) e.g. commercial notification and monitoring services

COMMERCIAL SERVICES (YES | NO) e.g. inclusion in commercial information feeds

NON COMMERCIAL USE

CUSTOMER NOTIFICATIONS (YES | NO) e.g. service provider informing customer of a potential issue

RESEARCH (YES | NO) e.g. research into threat groups or analytics of trends

TERMS OF USE

Description, summary, or references to any applicable licenses, agreements, or conditions between the producer and receiver

Join the discussion!

Information Exchange Policy Framework

Industry discussion, consensus and collaboration is needed to get it right, and gain wide spread support and adoption

The framework will be released under FIRST, the Forum for Incident Response Security Teams (www.first.org)

The framework development will be coordinated through a FIRST Special Interest Group

Non-FIRST members can participate and contribute to this SIG

FIRST Special Interest Group Goals and Objectives

1. Improve the ability for organizations to convey and interpret policy associated with exchanging security and threat information
2. Develop and publish an extensible information exchange policy framework
3. Develop and publish a set of common definitions for the framework and as a stand along reference for developing policies and sharing agreements

Question Time!

Merike Kaeo - merike@doubleshotsecurity.com

Paul McKitrick - pmckit@microsoft.com