Threat-Based “Cyber Operations Rapid Assessment” (CORA)

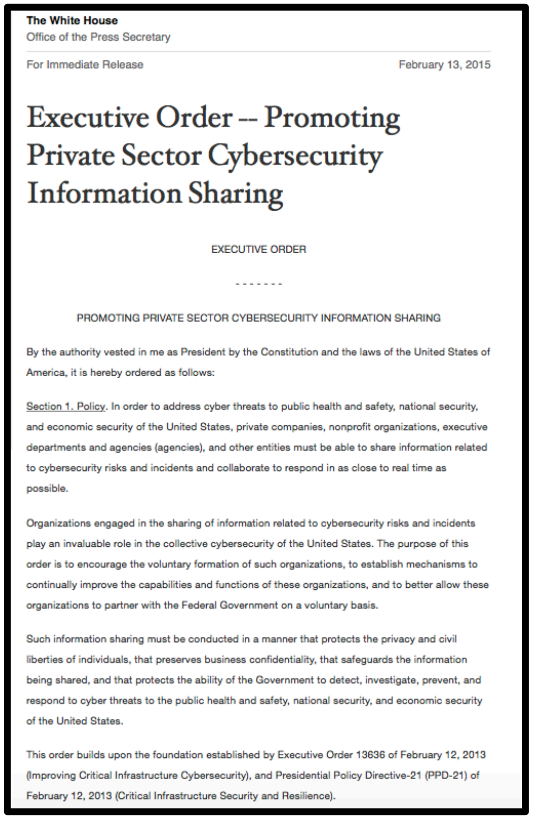
2015 Cyber Innovation Forum
September 9-11, 2015

POC: Dr. Lindsley Boiney

lboiney@mitre.org

Approved for Public Release; Distribution Unlimited. Case Number 15-2570

Cybersecurity Information Sharing…



The White House
Office of the Press Secretary

For Immediate Release — February 13, 2015

Executive Order -- Promoting Private Sector Cybersecurity Information Sharing

EXECUTIVE ORDER

- - - - - - -

PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

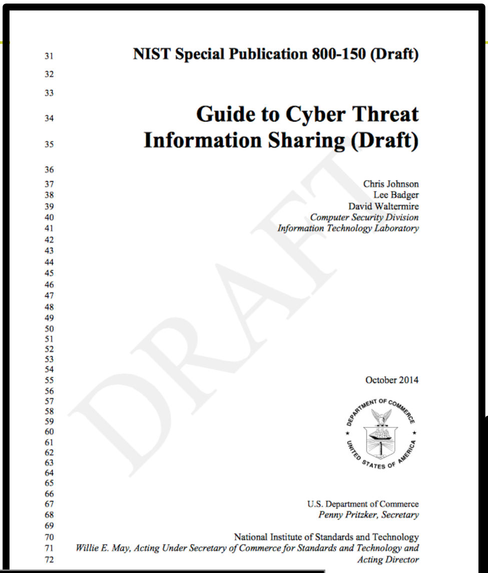
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience).



NIST Special Publication 800-150 (Draft)

Guide to Cyber Threat Information Sharing (Draft)

Chris Johnson
Lee Badger
David Waltermire
Computer Security Division
Information Technology Laboratory

DRAFT

October 2014

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA

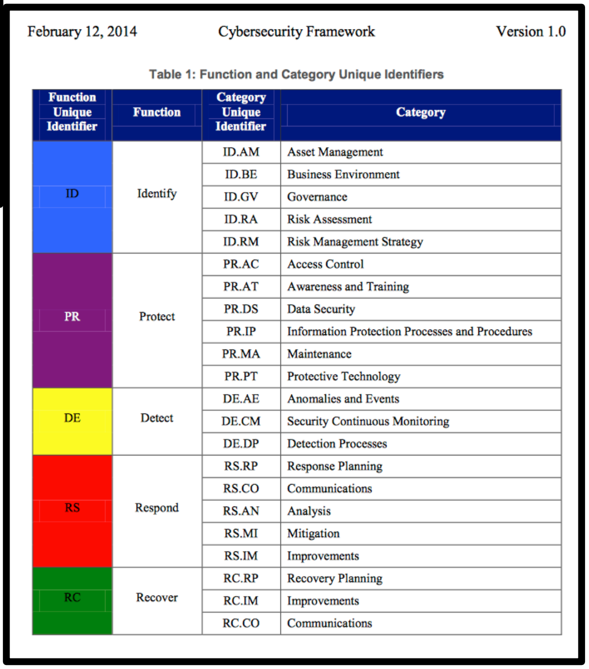
U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie E. May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

MITRE

Ten Strategies of a World-Class
Cybersecurity Operations Center

Carson Zimmerman



February 12, 2014 — Cybersecurity Framework — Version 1.0

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Problem

Many organizations are behind the curve in terms of threat intelligence, relying predominantly on static defensive measures and compliance-oriented processes. Transitioning to a “threat-oriented” posture is not easy, and change needs to occur across the triad of people, processes and technologies.

How can we address the gaps,
help organizations move forward?

Background

- The methodology grew out of MITRE research to explore how cyber threat information is
  - *collected*
  - *utilized*
  - *shared*

- Research Questions
  - What are an organization's cyber threat sharing and utilization capabilities?
  - What is a threat-sharing community's landscape?
  - What are facilitators/impediments to threat sharing?

Approved for Public Release; Distribution Unlimited. Case Number 15-2570

Approach – Practical and Doable

- An interactive engagement, more than an assessment
  - Solicit input and feedback from participants
  - Leverage MITRE role as independent third party
- Survey takes 2 hours to complete
  - Typically CISO, Security Operations Manager
- Followed by a semi-structured interview of 2 hours
  - Questions reviewed, discussed in more detail
- Analysis phase
- Participant receives 8-slide summary report
  - Strengths, Opportunities for Improvement, Capabilities, Recommendations

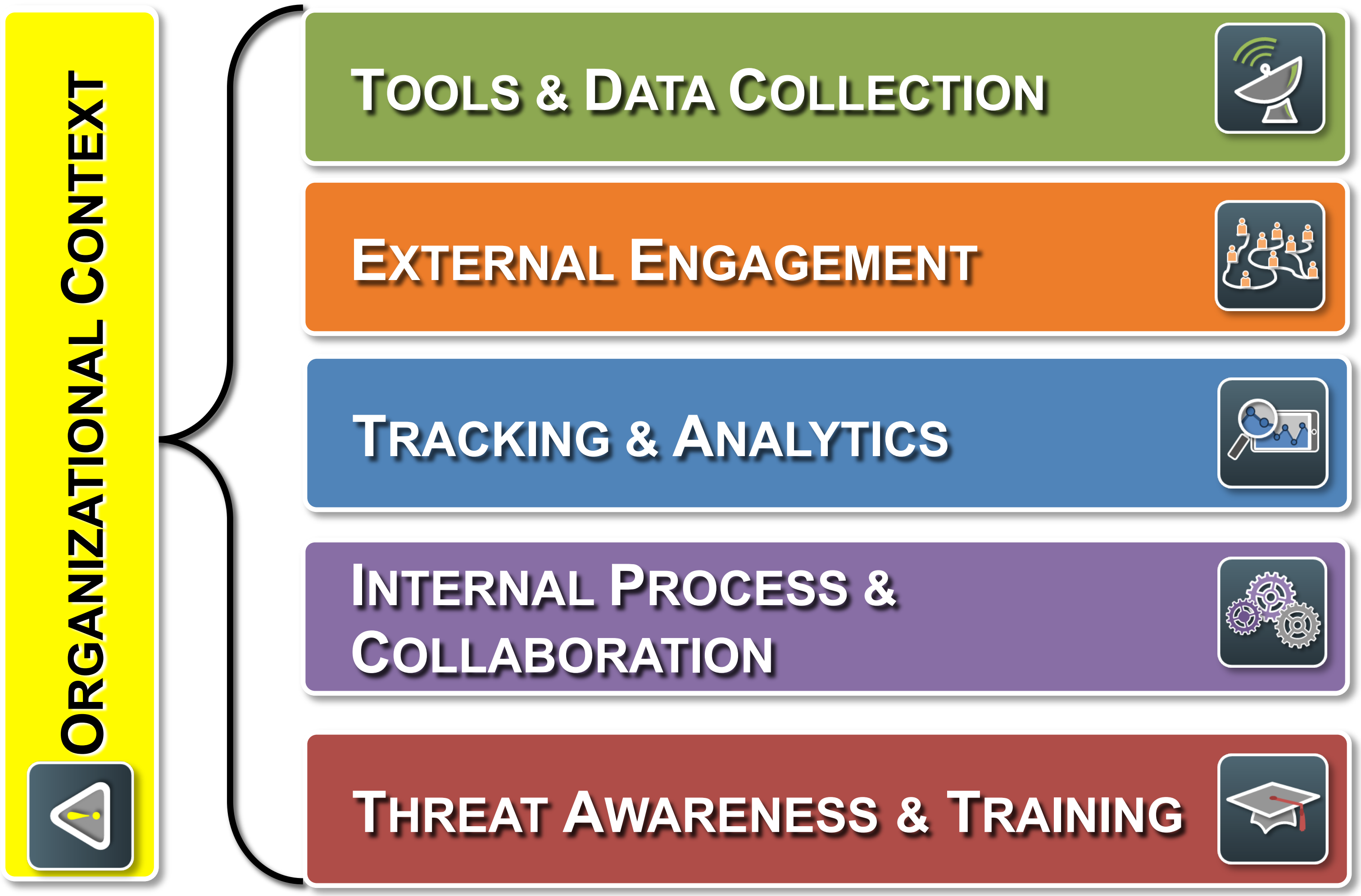
Piloted Through Multiple Engagements

- Piloted effectively with organizations (additional engagements in progress)
  - Sizes ranging from a few hundred to 100,000+ employees
  - Public and Private sectors
  - Industry sectors including financial, information technology, and healthcare

- Provide individual reports to participating organizations, with tailored recommendations as appropriate

- Provide summary briefing to group of participants, when applicable, on high-level findings and overall landscape

CORA Focus Areas



ORGANIZATIONAL CONTEXT

TOOLS & DATA COLLECTION

EXTERNAL ENGAGEMENT

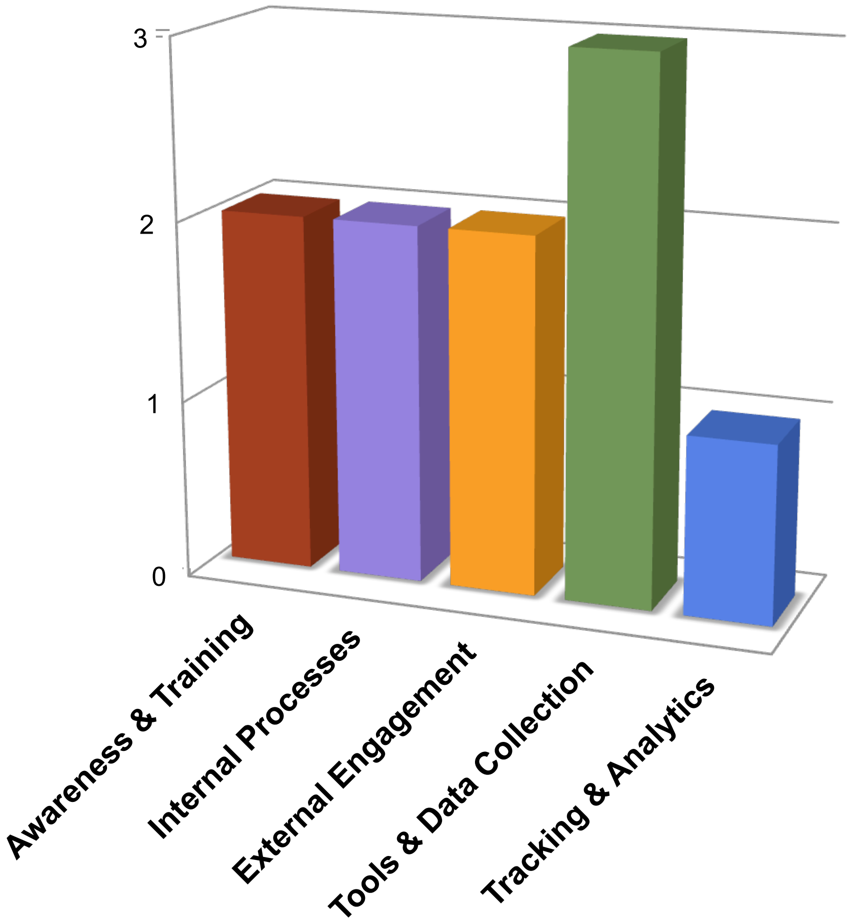
TRACKING & ANALYTICS

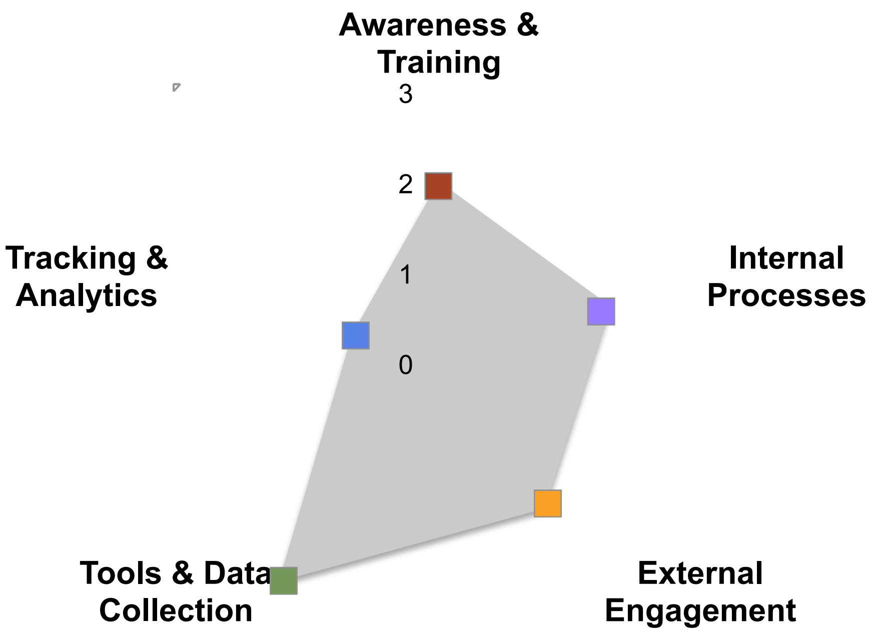
INTERNAL PROCESS & COLLABORATION

THREAT AWARENESS & TRAINING

Approved for Public Release; Distribution Unlimited. Case Number 15-2570

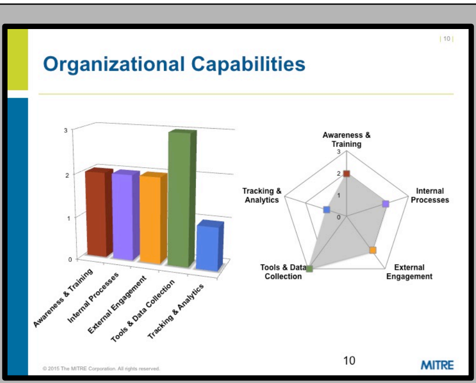
Ex: An Organization’s Capabilities





Approved for Public Release; Distribution Unlimited. Case Number 15-2570

What Do Results Look Like?

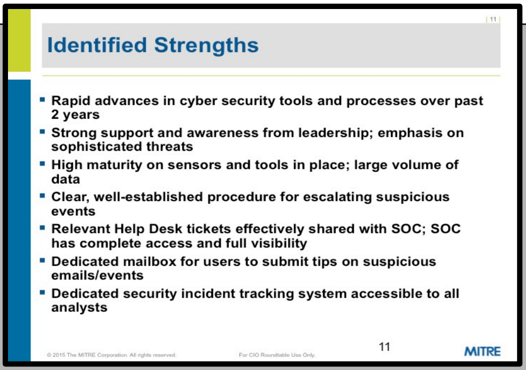


Organizational Capabilities

© 2015 The MITRE Corporation. All rights reserved.

10

MITRE



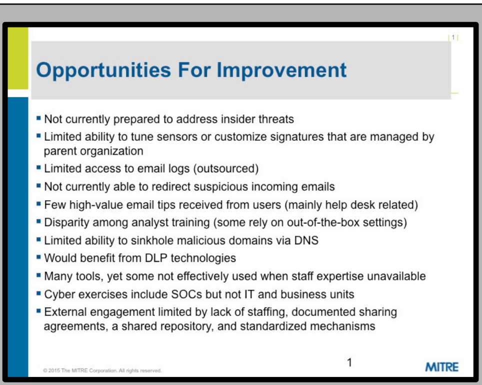
Identified Strengths

- Rapid advances in cyber security tools and processes over past 2 years
- Strong support and awareness from leadership; emphasis on sophisticated threats
- High maturity on sensors and tools in place; large volume of data
- Clear, well-established procedure for escalating suspicious events
- Relevant Help Desk tickets effectively shared with SOC; SOC has complete access and full visibility
- Dedicated mailbox for users to submit tips on suspicious emails/events
- Dedicated security incident tracking system accessible to all analysts

© 2015 The MITRE Corporation. All rights reserved. For CIO Roundtable Use Only

11

MITRE



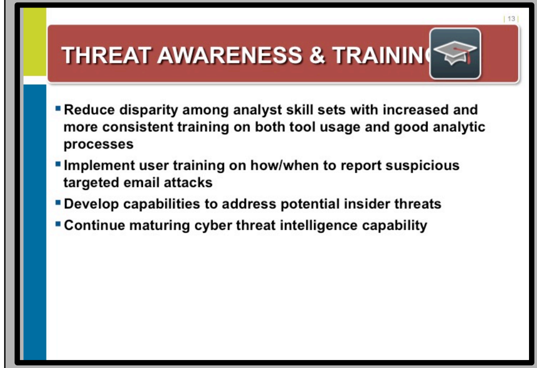
Opportunities For Improvement

- Not currently prepared to address insider threats
- Limited ability to tune sensors or customize signatures that are managed by parent organization
- Limited access to email logs (outsourced)
- Not currently able to redirect suspicious incoming emails
- Few high-value email tips received from users (mainly help desk related)
- Disparity among analyst training (some rely on out-of-the-box settings)
- Limited ability to sinkhole malicious domains via DNS
- Would benefit from DLP technologies
- Many tools, yet some not effectively used when staff expertise unavailable
- Cyber exercises include SOCs but not IT and business units
- External engagement limited by lack of staffing, documented sharing agreements, a shared repository, and standardized mechanisms

© 2015 The MITRE Corporation. All rights reserved.

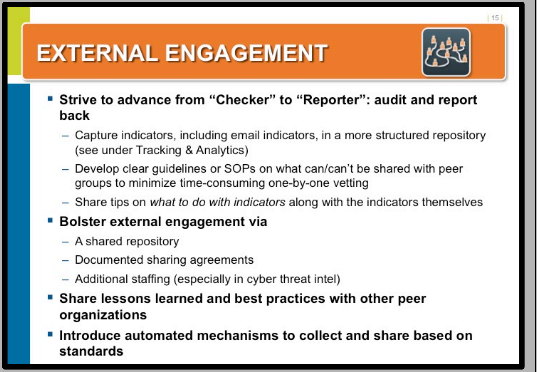
1

MITRE



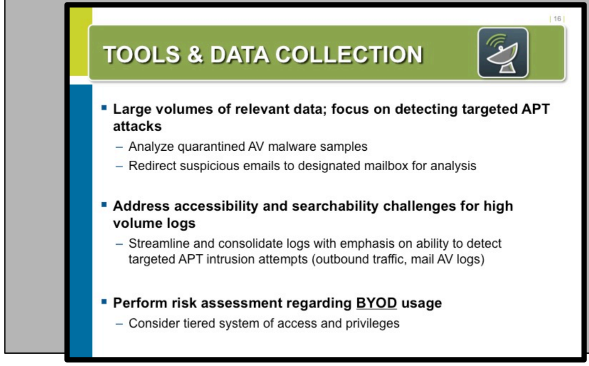
THREAT AWARENESS & TRAINING

- Reduce disparity among analyst skill sets with increased and more consistent training on both tool usage and good analytic processes
- Implement user training on how/when to report suspicious targeted email attacks
- Develop capabilities to address potential insider threats
- Continue maturing cyber threat intelligence capability



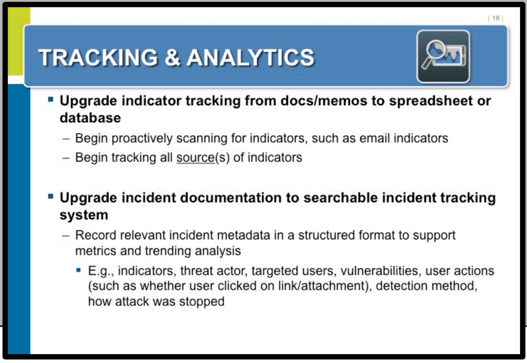
EXTERNAL ENGAGEMENT

- Strive to advance from "Checker" to "Reporter": audit and report back
  - Capture indicators, including email indicators, in a more structured repository (see under Tracking & Analytics)
  - Develop clear guidelines or SOPs on what can/can't be shared with peer groups to minimize time-consuming one-by-one vetting
  - Share tips on *what to do with indicators* along with the indicators themselves
- Bolster external engagement via
  - A shared repository
  - Documented sharing agreements
  - Additional staffing (especially in cyber threat intel)
- Share lessons learned and best practices with other peer organizations
- Introduce automated mechanisms to collect and share based on standards



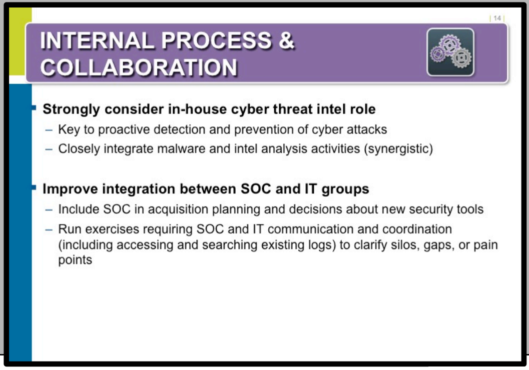
TOOLS & DATA COLLECTION

- Large volumes of relevant data; focus on detecting targeted APT attacks
  - Analyze quarantined AV malware samples
  - Redirect suspicious emails to designated mailbox for analysis
- Address accessibility and searchability challenges for high volume logs
  - Streamline and consolidate logs with emphasis on ability to detect targeted APT intrusion attempts (outbound traffic, mail AV logs)
- Perform risk assessment regarding BYOD usage
  - Consider tiered system of access and privileges



TRACKING & ANALYTICS

- Upgrade indicator tracking from docs/memos to spreadsheet or database
  - Begin proactively scanning for indicators, such as email indicators
  - Begin tracking all source(s) of indicators
- Upgrade incident documentation to searchable incident tracking system
  - Record relevant incident metadata in a structured format to support metrics and trending analysis
    - E.g., indicators, threat actor, targeted users, vulnerabilities, user actions (such as whether user clicked on link/attachment), detection method, how attack was stopped



INTERNAL PROCESS & COLLABORATION

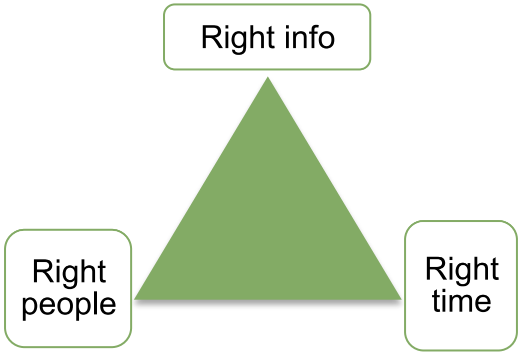
- Strongly consider in-house cyber threat intel role
  - Key to proactive detection and prevention of cyber attacks
  - Closely integrate malware and intel analysis activities (synergistic)
- Improve integration between SOC and IT groups
  - Include SOC in acquisition planning and decisions about new security tools
  - Run exercises requiring SOC and IT communication and coordination (including accessing and searching existing logs) to clarify silos, gaps, or pain points

Approved for Public Release; Distribution Unlimited. Case Number 15-2570

Some Findings:
TOOLS & DATA COLLECTION

Important distinctions less about particular tools and data quantity than about how interwoven with goals/processes

- **Don’t necessarily need more tools/information**
- **Gear collection toward primary threats (“right info”)**
  - Ex: external mail & AV logs, outbound traffic
  - Ex: suspicious email tips from users
- **Emphasize accessibility of logs (“to right people”)**
  - Are logs fed to SIEM, or must log in to access, or must fill out form/ticket, or beg and plead
  - Who owns which functions/logs (cyber security, IT, business unit, outsourced)
- **Emphasize searchability of logs (“at right time”)**
  - Time and effort to find what you need

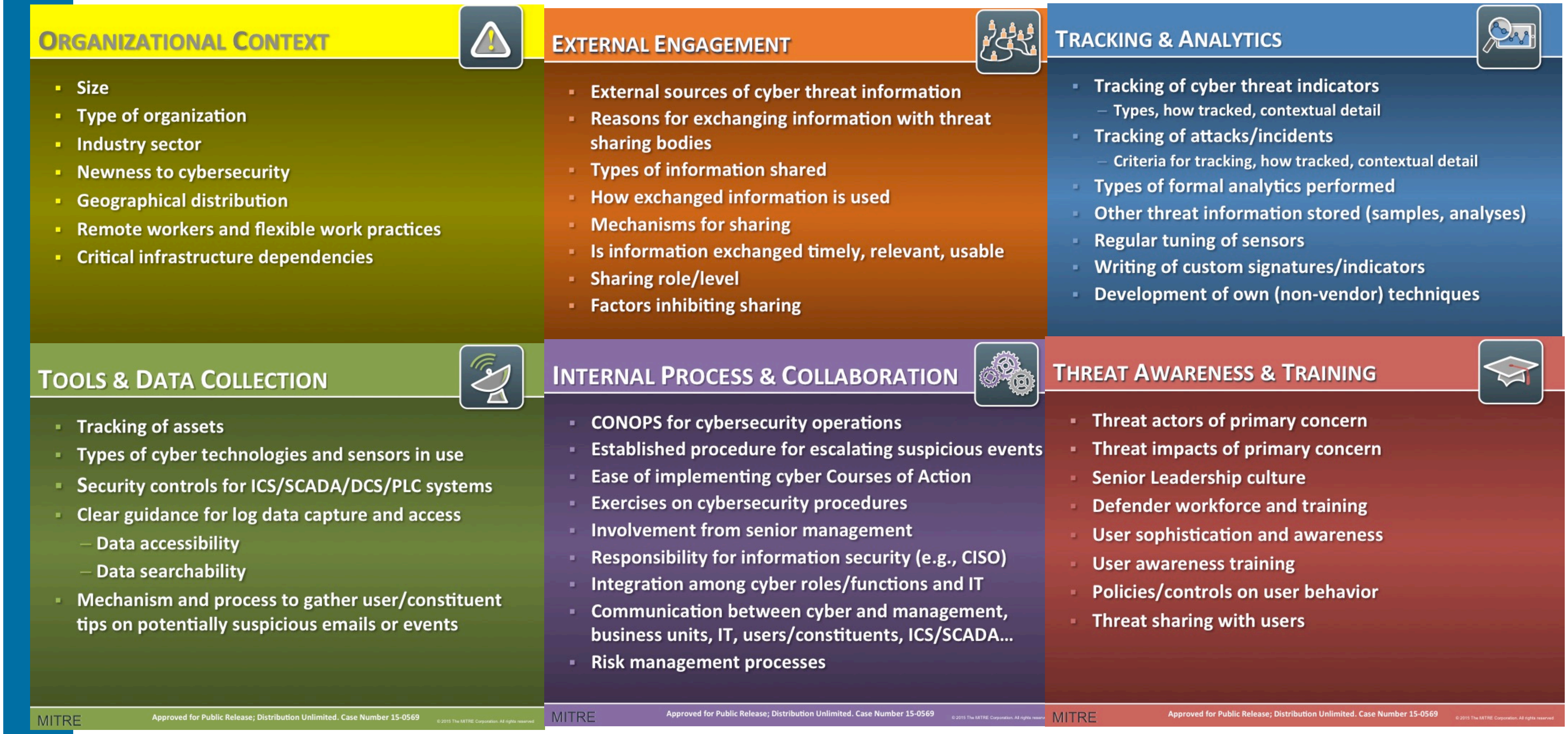


Approved for Public Release; Distribution Unlimited. Case Number 15-2570

Sample Recommendations: TOOLS & DATA COLLECTION

- **Large volumes of relevant data; focus on detecting targeted APT attacks**
  - Analyze quarantined AV malware samples
  - Redirect suspicious emails to designated mailbox for analysis
- **Address accessibility and searchability challenges for high volume logs**
  - Streamline and consolidate logs with emphasis on ability to detect targeted APT intrusion attempts (outbound traffic, mail AV logs)
- **Perform risk assessment regarding BYOD usage**
  - Consider tiered system of access and privileges

Content of Assessment Dimensions



Organizational Context

- Size
- Type of organization
- Industry sector
- Newness to cybersecurity
- Geographical distribution
- Remote workers and flexible work practices
- Critical infrastructure dependencies

External Engagement

- External sources of cyber threat information
- Reasons for exchanging information with threat sharing bodies
- Types of information shared
- How exchanged information is used
- Mechanisms for sharing
- Is information exchanged timely, relevant, usable
- Sharing role/level
- Factors inhibiting sharing

Tracking & Analytics

- Tracking of cyber threat indicators
  - Types, how tracked, contextual detail
- Tracking of attacks/incidents
  - Criteria for tracking, how tracked, contextual detail
- Types of formal analytics performed
- Other threat information stored (samples, analyses)
- Regular tuning of sensors
- Writing of custom signatures/indicators
- Development of own (non-vendor) techniques

Tools & Data Collection

- Tracking of assets
- Types of cyber technologies and sensors in use
- Security controls for ICS/SCADA/DCS/PLC systems
- Clear guidance for log data capture and access
  - Data accessibility
  - Data searchability
- Mechanism and process to gather user/constituent tips on potentially suspicious emails or events

Internal Process & Collaboration

- CONOPS for cybersecurity operations
- Established procedure for escalating suspicious events
- Ease of implementing cyber Courses of Action
- Exercises on cybersecurity procedures
- Involvement from senior management
- Responsibility for information security (e.g., CISO)
- Integration among cyber roles/functions and IT
- Communication between cyber and management, business units, IT, users/constituents, ICS/SCADA…
- Risk management processes

Threat Awareness & Training

- Threat actors of primary concern
- Threat impacts of primary concern
- Senior Leadership culture
- Defender workforce and training
- User sophistication and awareness
- User awareness training
- Policies/controls on user behavior
- Threat sharing with users

MITRE Approved for Public Release; Distribution Unlimited. Case Number 15-0569

MITRE Approved for Public Release; Distribution Unlimited. Case Number 15-0569

MITRE Approved for Public Release; Distribution Unlimited. Case Number 15-0569

Approved for Public Release; Distribution Unlimited. Case Number 15-2570

MITRE

External Engagement

- External sources of cyber threat information
- Reasons for exchanging information with threat sharing bodies
- Types of information shared
- How exchanged information is used
- Mechanisms for sharing
- Is information exchanged timely, relevant, usable
- Sharing role/level
- Factors inhibiting sharing

Some Findings:
EXTERNAL ENGAGEMENT

Q. Which of the options below best describes your organization's role in the threat sharing group?

○ **Member**: We receive reported threat information for our situational awareness

○ **Checker**: We scan our networks for reported threats, but don't report findings

○ **Reporter**: We scan our networks for reported threats, and also report back our findings

○ **Contributor**: We scan for reported threats and sometimes identify and share additional threat information

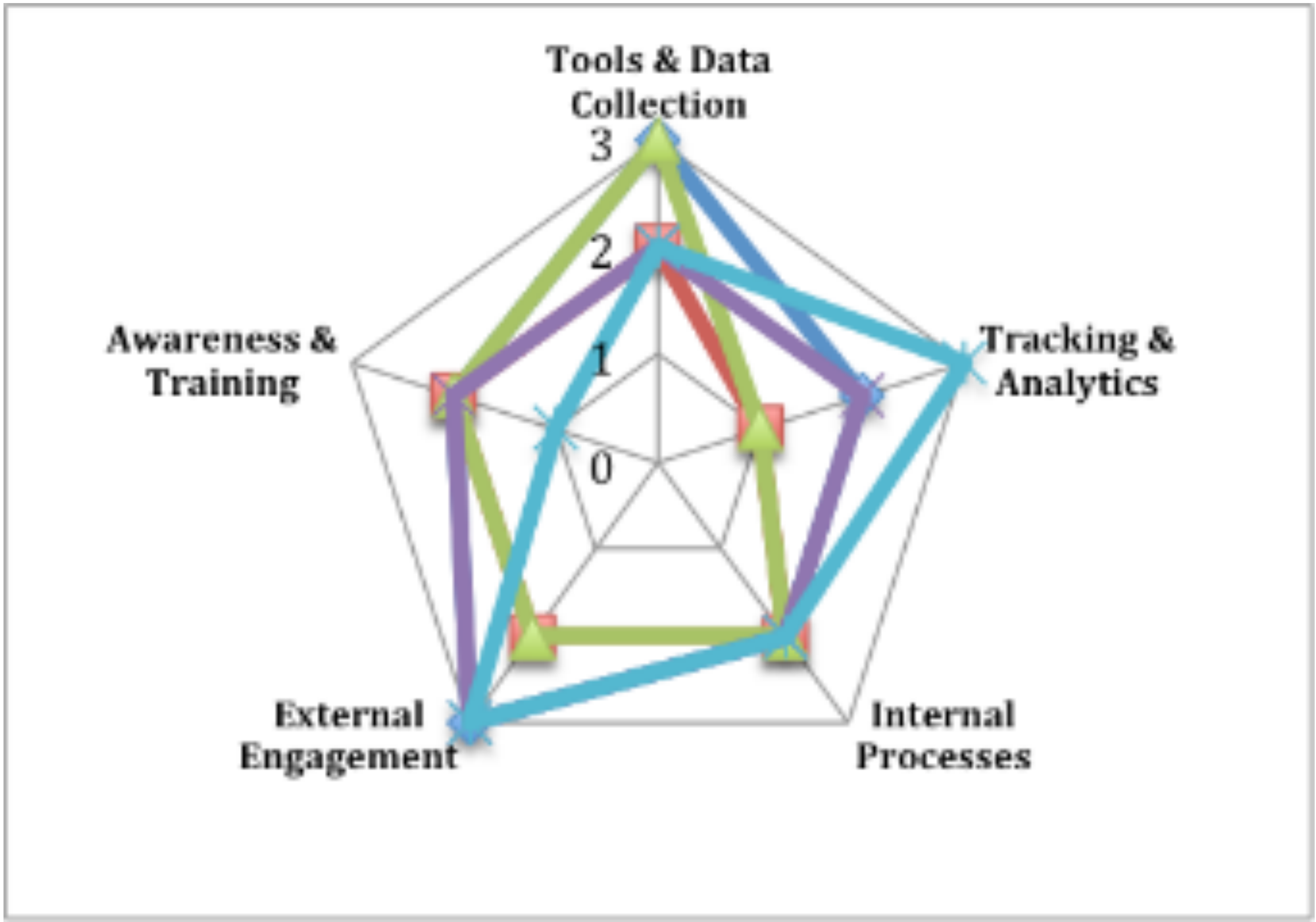
○ **Leader**: We scan for reported threats and are a regular and primary contributor of trusted threat information

- **Most are Members or Checkers: Checker v. Reporter key distinguisher!**
- **Challenges relate to**
  - Technology (ingesting/tracking)
  - Process (policy/vetting)
  - People (cyber threat intelligence analyst)

Sample Recommendations: EXTERNAL ENGAGEMENT

- **Strive to advance from “Checker” to “Reporter”: audit and report back**
  - Capture indicators, including email indicators, in a more structured repository
  - Develop clear guidelines or SOPs on what can/can’t be shared with peer groups to minimize time-consuming one-by-one vetting
  - Share tips on *what to do with indicators* along with the indicators themselves
- **Bolster external engagement via**
  - A shared repository
  - Documented sharing agreements
  - Additional staffing (especially in cyber threat intelligence)
- **Share lessons learned and best practices with other peer organizations**
- **Introduce automated mechanisms to collect and share based on standards**

Also: Landscape For a Group (e.g., ISAC)



Approved for Public Release; Distribution Unlimited. Case Number 15-2570

Sample Recommendations (all areas)

- Gain access to perimeter email logs
- Address accessibility and searchability challenges for logs
  - emphasis on detecting targeted attempts (outbound traffic, mail AV logs)
- Upgrade indicator tracking from docs/memos to database
  - Email indicators: “redirect” suspicious incoming emails to analyst mailbox
- Use signatures from peers to proactively scan for APT indicators
- Consider in-house cyber threat intel role
- Strengthen integration between IT and cyber security groups via exercises, liaison roles, tech exchanges, joint planning decisions
- Strengthen controls on network usage (2 factor authentication, forced VPN)
- Perform risk assessment regarding BYOD usage
- Strengthen user awareness training: threat bulletins, *real* examples, what to do before you click, contests…*ongoing* campaign
- Strive to advance one level (e.g. “Checker” to “Reporter”)
- Consider sharing logs, samples (indicators aren’t the only valuable data)

Impact

- Guide organizations through structured review of a broad range of issues necessary to support threat-based operations
- Rapidly assess threat-oriented cyber security capabilities
- Raise awareness, focus attention and resources to improve cyber operations
- Provide timely, unbiased, actionable guidance to share with senior management
- Help threat sharing bodies understand the capabilities of their members and improve services and activities

Some Other Assessments

- Hewlett Packard Security Operations Maturity Assessment
- Kroll Cyber Risk Assessment
- Coalfire Cyber Risk and Controls Assessments
- Mandiant Response Readiness Assessment
- Booz Allen Cyber Operations Maturity Framework
- NetDiligence QuietAudit Cyber Risk Assessment

- DHS US-CERT Cyber Resilience Review
- DHS Cyber Security Evaluation Tool
- DHS Cybersecurity Assessment and Risk Management Approach
- CANSO Cyber Security and Risk Assessment Guide

- SANS Baseline, Audit and Assess, Secure, Evaluate and Educate Assessment Methodology
- Software Engineering Institute OCTAVE Allegro
- QuERIES Quantitative Evaluation of Risk for Investment Efficient Strategies

What sets CORA apart?

- Rapid
- Unbiased
- Focus on threat sharing
- Interactive
- Actionable guidance

Approved for Public Release; Distribution Unlimited. Case Number 15-2570

Setting Expectations

- **What the CORA methodology DOES NOT do**
  - Impose requirements or mandate responses
  - Address regulatory and compliance issues (e.g., FISMA, PCI DSS, SOX)
  - Require access to organizational logs/systems (no vulnerability assessment or pen testing)
  - Reveal sensitive data to others
  - Recommend vendor-specific tools/sensors/services
  - Perform an architectural assessment
  - Provide detailed technical guidance

Next Steps

- **Study more organizations / collect more data for evidence-based analytics and recommendations**
  - Transition to sponsor work programs
  - Tailor for threat sharing bodies such as ISACs, ISAOs, Federal Cyber Operation Centers
- **Develop analytics**
  - Metrics
  - Link CORA recommendations to existing resources
- **Identify and share best practices and use cases**
  - What works or doesn't work well? In which cases?

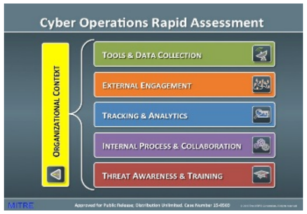
Threat-Based "Cyber Operations Rapid Assessment" (CORA)

Problem

Many organizations are behind the curve in terms of threat intelligence, relying predominantly on static defensive measures and compliance-oriented processes. Transitioning to a "threat-oriented" posture is not easy, and change needs to occur across the triad of people, processes and technologies.

Idea

MITRE has developed and piloted a **Cyber Operations Rapid Assessment** (CORA) methodology, to identify areas in cyber security defensive practices where improvements can be made in the *collection*, *utilization*, and *sharing* of *threat intelligence*.



Cyber Operations Rapid Assessment

Organizational Context

Tools & Data Collection

External Engagement

Tracking & Analytics

Internal Process & Collaboration

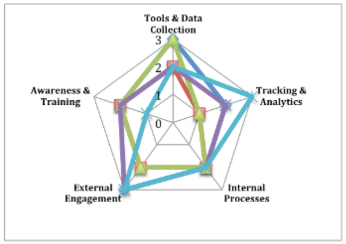
Threat Awareness & Training

MITRE

Approved for Public Release; Distribution Unlimited. Case Number 15-0565

Findings

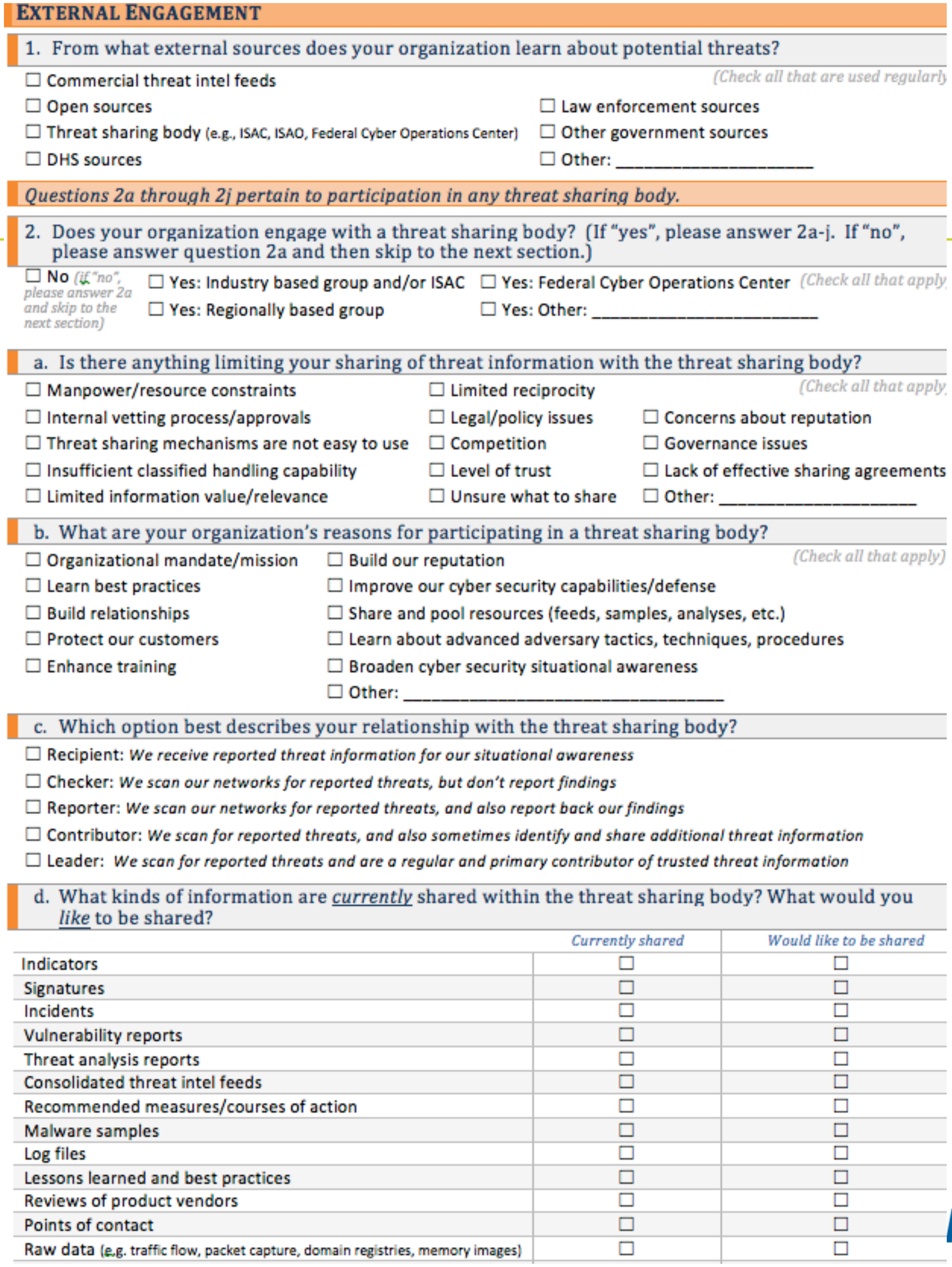
The CORA methodology is applicable to organizations of different sizes, industries, and capabilities. It has been used to identify focus areas for improving threat intelligence utilization and exchange. Key discriminators include log data accessibility and searchability, indicator and incident tracking, leadership threat awareness, and integration between IT and cyber groups.



Impacts

- Rapidly assess threat-oriented cyber security capabilities
- Help tailor work programs to improve cyber operations
- Help threat information sharing bodies understand members capabilities and improve services
- Improve Cyber Operations effectiveness

BACKUPS



External Engagement

1. From what external sources does your organization learn about potential threats?

(Check all that are used regularly

☐ Commercial threat intel feeds

☐ Open sources

☐ Threat sharing body (e.g., ISAC, ISAO, Federal Cyber Operations Center)

☐ DHS sources

☐ Law enforcement sources

☐ Other government sources

☐ Other: ____________________

Questions 2a through 2j pertain to participation in any threat sharing body.

2. Does your organization engage with a threat sharing body? (If "yes", please answer 2a-j. If "no", please answer question 2a and then skip to the next section.)

(Check all that apply

☐ No *(if "no", please answer 2a and skip to the next section)*

☐ Yes: Industry based group and/or ISAC

☐ Yes: Regionally based group

☐ Yes: Federal Cyber Operations Center

☐ Yes: Other: ______________________

a. Is there anything limiting your sharing of threat information with the threat sharing body?

(Check all that apply

☐ Manpower/resource constraints

☐ Internal vetting process/approvals

☐ Threat sharing mechanisms are not easy to use

☐ Insufficient classified handling capability

☐ Limited information value/relevance

☐ Limited reciprocity

☐ Legal/policy issues

☐ Competition

☐ Level of trust

☐ Unsure what to share

☐ Concerns about reputation

☐ Governance issues

☐ Lack of effective sharing agreements

☐ Other: ____________________

b. What are your organization's reasons for participating in a threat sharing body?

(Check all that apply)

☐ Organizational mandate/mission

☐ Learn best practices

☐ Build relationships

☐ Protect our customers

☐ Enhance training

☐ Build our reputation

☐ Improve our cyber security capabilities/defense

☐ Share and pool resources (feeds, samples, analyses, etc.)

☐ Learn about advanced adversary tactics, techniques, procedures

☐ Broaden cyber security situational awareness

☐ Other: ________________________________

c. Which option best describes your relationship with the threat sharing body?

☐ Recipient: *We receive reported threat information for our situational awareness*

☐ Checker: *We scan our networks for reported threats, but don't report findings*

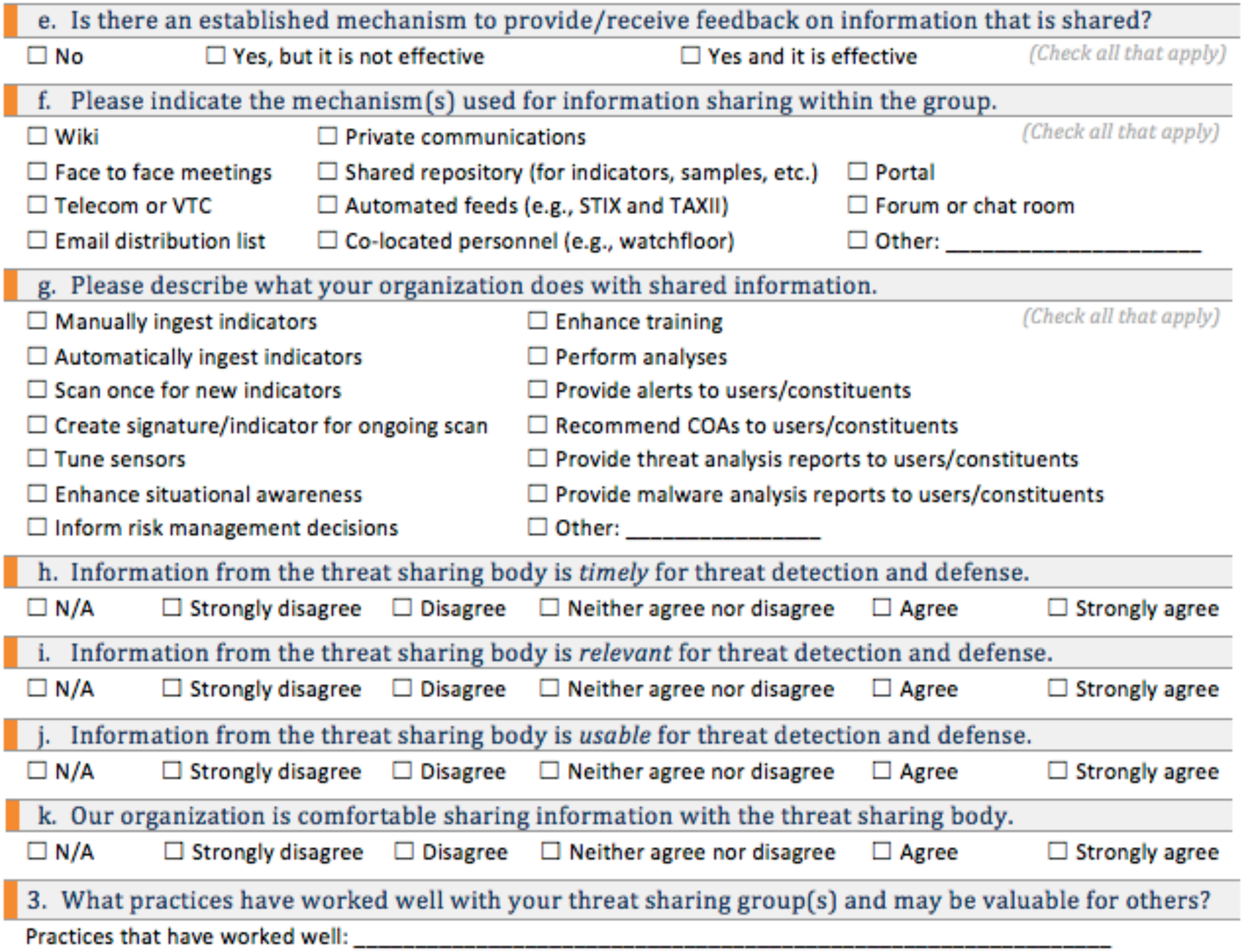
☐ Reporter: *We scan our networks for reported threats, and also report back our findings*

☐ Contributor: *We scan for reported threats, and also sometimes identify and share additional threat information*

☐ Leader: *We scan for reported threats and are a regular and primary contributor of trusted threat information*

d. What kinds of information are *currently* shared within the threat sharing body? What would you *like* to be shared?

	Currently shared	*Would like to be shared*
Indicators	☐	☐
Signatures	☐	☐
Incidents	☐	☐
Vulnerability reports	☐	☐
Threat analysis reports	☐	☐
Consolidated threat intel feeds	☐	☐
Recommended measures/courses of action	☐	☐
Malware samples	☐	☐
Log files	☐	☐
Lessons learned and best practices	☐	☐
Reviews of product vendors	☐	☐
Points of contact	☐	☐
Raw data (e.g. traffic flow, packet capture, domain registries, memory images)	☐	☐



e. Is there an established mechanism to provide/receive feedback on information that is shared?

☐ No ☐ Yes, but it is not effective ☐ Yes and it is effective *(Check all that apply)*

f. Please indicate the mechanism(s) used for information sharing within the group.

(Check all that apply)

☐ Wiki

☐ Face to face meetings

☐ Telecom or VTC

☐ Email distribution list

☐ Private communications

☐ Shared repository (for indicators, samples, etc.)

☐ Automated feeds (e.g., STIX and TAXII)

☐ Co-located personnel (e.g., watchfloor)

☐ Portal

☐ Forum or chat room

☐ Other: ____________________

g. Please describe what your organization does with shared information.

(Check all that apply)

☐ Manually ingest indicators

☐ Automatically ingest indicators

☐ Scan once for new indicators

☐ Create signature/indicator for ongoing scan

☐ Tune sensors

☐ Enhance situational awareness

☐ Inform risk management decisions

☐ Enhance training

☐ Perform analyses

☐ Provide alerts to users/constituents

☐ Recommend COAs to users/constituents

☐ Provide threat analysis reports to users/constituents

☐ Provide malware analysis reports to users/constituents

☐ Other: ________________

h. Information from the threat sharing body is *timely* for threat detection and defense.

☐ N/A ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

i. Information from the threat sharing body is *relevant* for threat detection and defense.

☐ N/A ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

j. Information from the threat sharing body is *usable* for threat detection and defense.

☐ N/A ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

k. Our organization is comfortable sharing information with the threat sharing body.

☐ N/A ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

3. What practices have worked well with your threat sharing group(s) and may be valuable for others?

Practices that have worked well: ____

Goals

- Gather actual data to move beyond anecdotes and claims
- Generate *tailored guidance* rather than a score
- Raise organizational awareness of cyber capabilities by identifying strengths/challenges
- Uncover and promulgate best practices
- Capture a community's capability landscape
- Improve services and activities supporting cyber threat information utilization and exchange

CORA Methodology - Characteristics

- Lightweight (2 hours survey, 2 hours interview)
- Threat-Focused (people, processes, technology)
- Unbiased feedback (tool/technology/service agnostic)
- Interactive (neither *Do-It-Yourself* nor *Done-Unto-You*)
- Applicable to organizations across a broad spectrum of sizes, sectors, and capabilities
- Actionable guidance