Extending Your Human Sensor Network: Measurable Threat Defense

Ellen Powers

18 August 2015
Filling the Gap in Cyber Defense for the Advanced Threat

- Log Analysis
- Block prevention
- Human Sensors
- Sensor detection
- Cyber Intelligence
Threat Awareness Today

- Human Sensors
- Targets
- Clickers

Focus

Increase

decrease
Threat instigates Human Sensor Network

**Bang!**
- Gap analysis
- Executive action

**Ready**
- Tell the story
- Provide opportunity

**Engage**
- Respond
- Recognize

 Measure!
Bang!

- **Gap analysis**
  - Ask your cyber operations team
    - What gets through?
    - What is the scale of concern?
    - Where/Who are most at-risk?
# Cyber Threat Landscape Highlight

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Vulnerabilities</th>
<th>Threats</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Internet-enabled and exposed applications</td>
<td>Cyber Crime, Hacktivists, Advanced Persistent Threat (APT)</td>
<td>Web-based (e.g., drive-by; fake A/V; plug-in’s) Email-based (phishing, spear-phishing, whaling)</td>
</tr>
<tr>
<td>People</td>
<td>Curiosity, Haste, Fear, Technology inexperience, Technical illiteracy, Cognitive dissonance</td>
<td>“Game of wits”</td>
<td></td>
</tr>
</tbody>
</table>

The advanced cyber adversary needs only one click with “right” conditions.
Gap Analysis

TIP: Use a spreadsheet to jump start analysis

- Subjects/themes?
- Links/attachments?
- New target/known target?
- Reporter? Clicker?
- Threat actor groupings?
Post Mortem Gap Analysis with Human Sensors

11:30 AM
Attack begins
Credible link

12:50 PM
Email Reported

1:20 PM
M&R Response

2:30 PM
Sensor detection
Containment

4:00 PM
Target Threat Alert

Human sensor
opportunity

TAKE-AWAY
Use your threat landscape and attack data to focus your threat awareness program.

Measure!
Bang!

- **Gap analysis**
  - Ask your cyber operations team
    - What gets through?
    - What is the scale of concern?
    - Where/Who are most at-risk?

- **Executive action**
  - Aha moment
    - Qualify your threat landscape
    - Show the means of attack
    - Change the game
# Aha Moment: Example Means of Attack

## Opportunity for employees to be cyber defenders and human sensors.

<table>
<thead>
<tr>
<th>Event</th>
<th>0-day Date</th>
<th>Patch Issued</th>
<th>Initial Attack</th>
<th>Other Attack</th>
<th>90% Compliance Date</th>
<th>Other Attack</th>
<th>Other Attack</th>
<th>Other Attack</th>
</tr>
</thead>
</table>

*Measure!*
Aha Moment: Example Risk Latency

Weekly % Non-Compliant

![Graph showing high and low points of risk over time.]

- **High-point of risk**
- **Low-point of risk**

Notional

Each peak shows risk not reduced as advised (missed deadline)

Each gap shows time to close known vulnerability

**Measure!**
Aha Moment: Executive action

Key to Success: Senior management begins monitoring patch compliance

80% of attacks can be mitigated by up-to-date patches*

Tell the story

- Your actual situation matters more than generalities
- Personal stories (with people you know!) have more impact
- Transparency builds trust $\rightarrow$ trust creates willingness $\rightarrow$ willingness seizes opportunity
Tell the Stories: Real Incidents

Social comparison as a basis for heightening threat awareness

Survey of Readers of MITRE True Stories

- Found them useful
- Would change future behavior

 Measure!
Ready

Tell the story
- Your actual situation matters more than generalities
- Personal stories (with people you know!) have more impact
- Transparency builds trust → trust creates willingness → willingness seizes opportunity

Provide opportunity
- How to report
- Learn detection method
- Safe practice
Opportunity: Report and Skill-building

- **Starter Method**
  - Email Self-questioning Technique
    - Expected?
    - Ambiguous?
    - Relationship?
    - Normal?
    - Exposed?
    - Sense?
    - Time?

- **Active Uncertainty Method**
  - Email SOS
    - Check Sender address and name
    - Hover Over the links
    - Determine if the messages makes Sense
Opportunity: Safe Practice

Uncovering Suspicious Email

Even though you decided one or more messages were legitimate, clicking a link or opening an attachment in such a message might compromise your system and MITRE. In this case, however, we were not compromised.

<table>
<thead>
<tr>
<th>#</th>
<th>Your answer</th>
<th>Correct answer</th>
<th>Result</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fake</td>
<td>Fake</td>
<td>✔️</td>
<td>Why?</td>
</tr>
<tr>
<td>2</td>
<td>Legitimate</td>
<td>Fake</td>
<td>✗</td>
<td>Why?</td>
</tr>
<tr>
<td>3</td>
<td>Don’t know</td>
<td>Legitimate</td>
<td>✗</td>
<td>Why?</td>
</tr>
<tr>
<td>4</td>
<td>Fake</td>
<td>Fake</td>
<td>✔️</td>
<td>Why?</td>
</tr>
<tr>
<td>5</td>
<td>Legitimate</td>
<td>Legitimate</td>
<td>✔️</td>
<td>Why?</td>
</tr>
<tr>
<td>6</td>
<td>Legitimate</td>
<td>Legitimate</td>
<td>✔️</td>
<td>Why?</td>
</tr>
</tbody>
</table>

Question 2

Conficker has the letter L when it should say Conficker, not L, the official name of the worm.

This appears to come from yourself, although the name says Microsoft Team.

An outbreak on MITRE’s network would not be communicated by Microsoft or any other vendor.

More information...

Fake 45% (5)
Legitimate 45% (5)
Don’t know 9% (1)
Total votes: 11

Measure!
Opportunity: Learn, Report, Detect

Suspicious Email Reporting

![Graph showing suspicious email reporting over time](image)

**Human Sensor Network: number of APT emails “discovered”**

- Before safe practice: 1
- After safe practice: 5

**TAKE-AWAY**

Build-in measurement for each focused “activity” and its effect.

**Measure!**
Engage

- Respond
  - Personalized responses
  - Focused alerting
  - Invitational and pro-active threat briefings
Respond: Personalized Response

- **Suspicious Triage process**
  - Personalized responses
  - Learning opportunity
  - Threat Awareness

- **Enable self-reporting**
  - Acknowledgement and appreciation rather than penalty
Respond: Focused Alerting

- Cyber Threat Alerts
  - Delivered and intercepted attacks
  - Pre-attack warnings to known targets
  - Phishing alerts

Email Sent to Targeted Employees

You are receiving this email because you are a target of an advanced cyber adversary.

An email with subject “[Redacted]” was intercepted on [Redacted] and not delivered to your inboxes.

The email was an attack by an advanced cyber adversary using the Flash 0-day vulnerability patch as a lure.

You can be a human sensor by reporting suspect email to sus[Redacted]org — sometimes a user report is the only alert we receive.

We appreciate your help defending your inbox and MITRE.

Best regards,

MITRE InfoSec Cyber Threat Awareness
For tips on defending your inbox, see FJ: learn email security
Respond: Threat Briefings

- Threat Readiness for
  - Targeted programs
  - At-risk groups (e.g., HR)

- Learn about Threat
  - What to look for
  - Indicators for post-click
  - How and where to report
Human Defensive Measures

Effectiveness of Our Human Sensors – Incidents Detected, Analyzed, and Deterred through Suspicious Email Reporting

Measure!

- Number of Incidents Detected by Suspicious Only
- Number of Suspicious Email Reports Submitted Only
- Number of Suspicious Email Reports Submitted for Malware Analysis

Every suspicious email reported requires email triage (purple line).
A portion of those reports are passed on for malware analysis (purple bar).
The green bar indicates the number of incidents that were detected as a result of the suspicious reporting, triage, and malware analysis.
Engage

- **Respond**
  - Personalized responses
  - Focused alerting
  - Invitational and pro-active threat briefings

- **Recognize**
  - Shout-outs
  - C-level kudos
Recognize: Shout-outs

- Phishing alerts acknowledge those who have reported
  - Shared responsibility for cyber defense
  - Shows how employee reporting makes a difference

Subject: Cyber Threat Alert for You
Importance: High

You help is needed.

Yesterday (Monday, July 11) you might have received an email message with a malicious .zip file attachment. The message had the following subject line:

"[Redacted]" (the subject line may vary).

Thanks to Robert [Redacted] and David [Redacted] for reporting this message to sus[Redacted]org thus giving us a chance to put in place defenses to protect MITRE from the cyber adversary.

If you clicked or opened the attachment, please let us know immediately so we can take action to protect MITRE.

As a precaution, if you received this message and haven't done so already, be sure to delete the message from your inbox, junk folder, and/or empty your trash folder.

We rely on you for MITRE's cyber defense, so please report any odd messages to sus[Redacted]org and any clicks that you regret or that do not do what you expect – doing so can help us stop a cyber attack. Please don't assume that any defense or sensor will detect or protect MITRE from the cyber adversary.

Please excuse this message if you already reported this message to sus[Redacted]org.

Best regards,

[Redacted]

MITRE InfoSec - Cyber Awareness Program
Recognize: Kudos for Human Sensor

- CSO recognizes individuals who report advanced threat email

**Thanks for your cyber vigilance**

Gagnon, Gary J.  
Wednesday, November 15 at 2:44 PM

To: Gary.J.Gagnon
Cc: Manager; He Supervisor; He Manager; By Division; By GM/VP

John

It has been brought to my attention that your report of a suspicious email on A,th turned out to be an attempt by an advanced persistent threat (APT). I would like to thank you for your prompt action in this matter--our employees are a key front-line of defense.

Thanks again for keeping us ahead of the game.

Gary Gagnon  
SVP and Chief Security Officer

**TAKE-AWAY**  
Personalization, appreciation, and recognition motivate willingness to report.
Human Sensor Evolution

- Delivered advanced threats
  - Reported?

- By threat actor
  - Human Sensor coverage?
    - E.g., 25% of known targets reported or 50% of a targeted attack reported

Measure!
Lessons Learned

- Reports to seniors aren’t sufficient for change
  - Executives need to hold them accountable for progress
- Don’t wait to get data from others
  - Request direct access or ask for your own feed
- Telling “bad” stories needs finesse
  - Even without attribution, inform those in the know ahead of publication
- Measurement influences results
  - Blind measurement or self measurement or social comparison: use the right one for your needs
- Partner with your threat and intelligence analysts
  - No surprises for them or you

Employees as cyber defenders, human sensors, and a source of cyber intelligence
Thank you!
Questions?