

How to Establish a Suspicious Email Program and Educate End Users

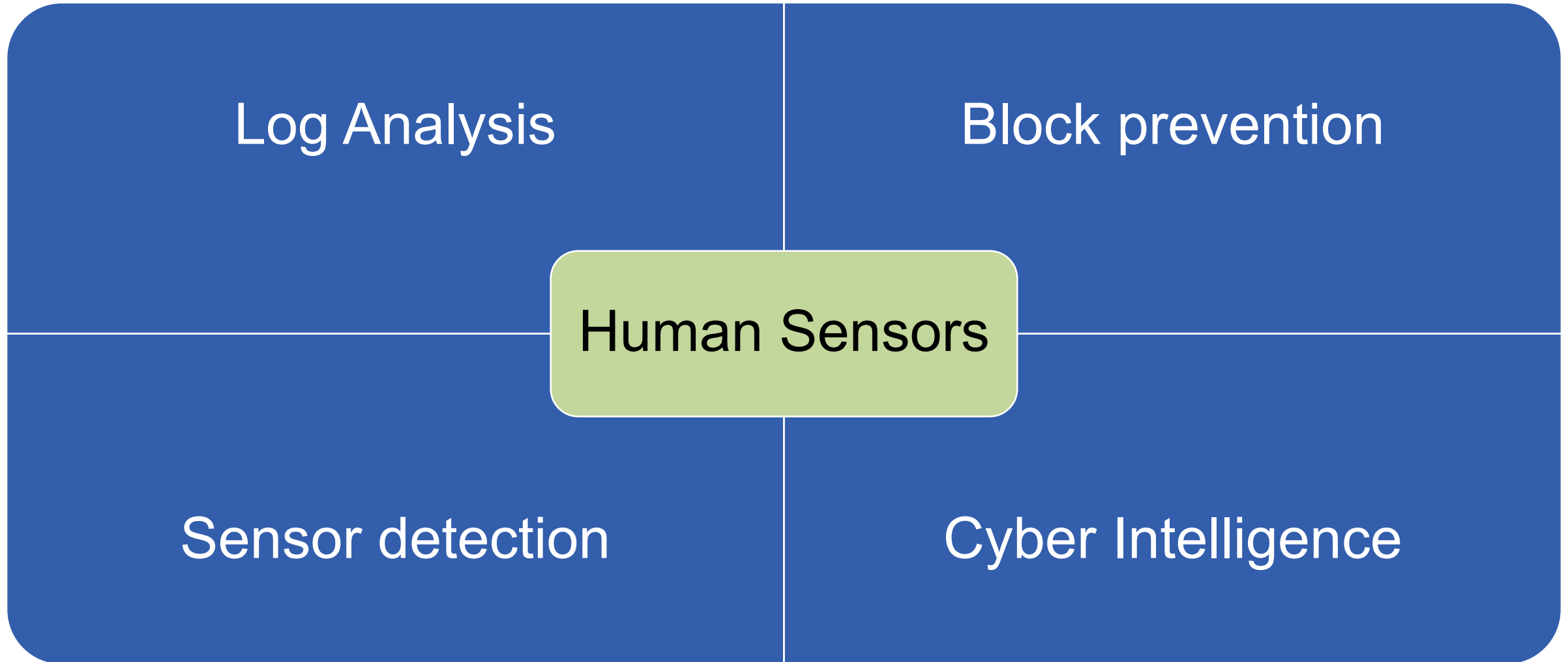
Ellen Powers

January 2021

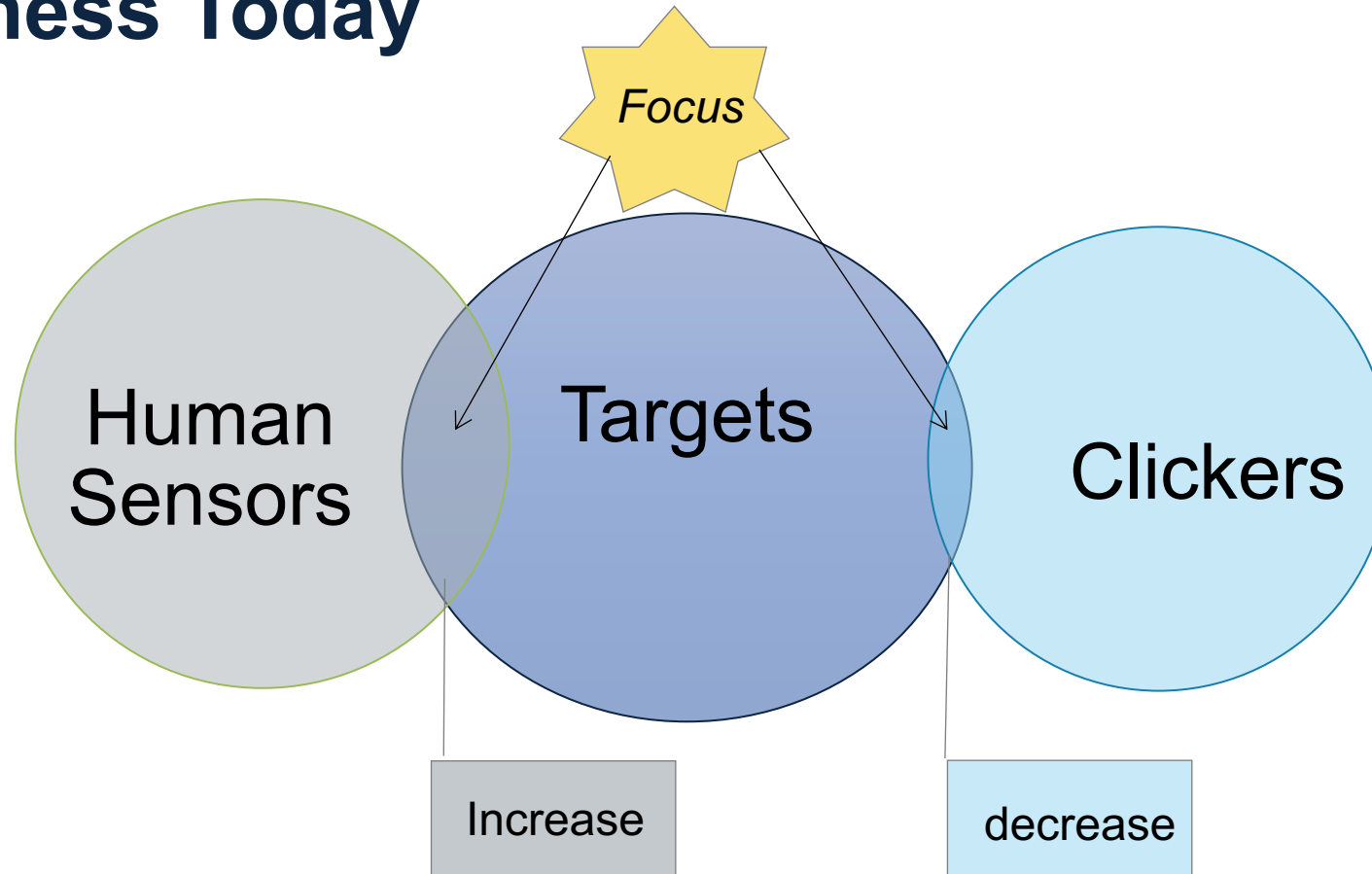
Suspicious Email Program Goal

**Employees as cyber defenders, human sensors,
and a source of cyber intelligence**

Filling the Gap in Cyber Defense for the Advanced Threat



Threat Awareness Today



Threat instigates Human Sensor Network



- Gap analysis
- Executive action



- Tell the story
- Provide opportunity



- Respond
- Recognize





Bang!

Gap analysis

Ask your cyber operations team

- What gets through?
- What is the scale of concern?
- Where/Who are most at-risk?

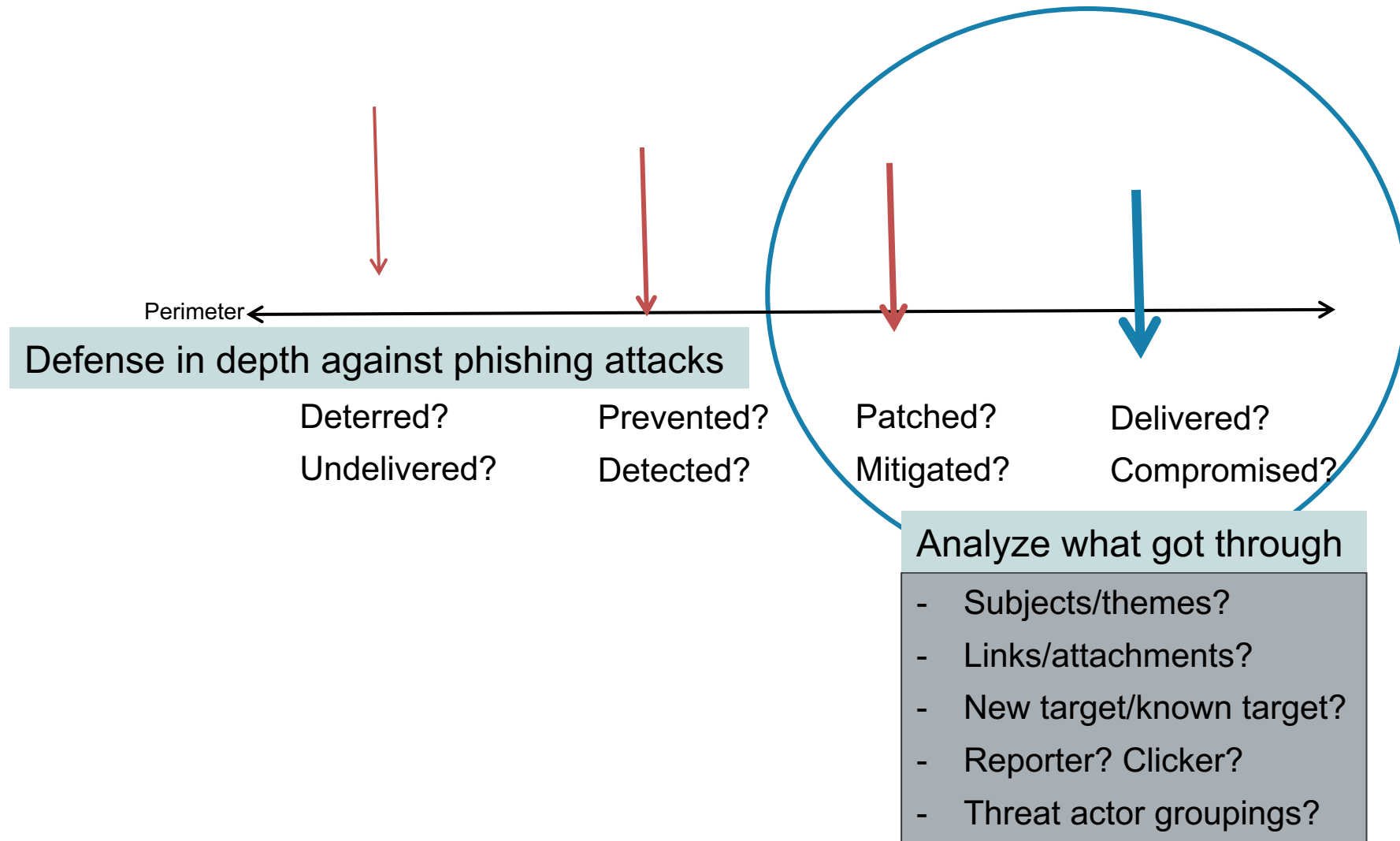
Cyber Threat Landscape Highlight

Attack Surface	Vulnerabilities	Threats	Attacks
Technology	Internet-enabled and exposed applications	Cyber Crime, Hacktivists, Advanced Persistent Threat (APT)	Web-based (e.g., drive-by; fake A/V; plug-in's) Email-based (phishing, spear-phishing, whaling)
People	Curiosity, Haste, Fear, Technology inexperience, Technical illiteracy, Cognitive dissonance		

“Game of wits”

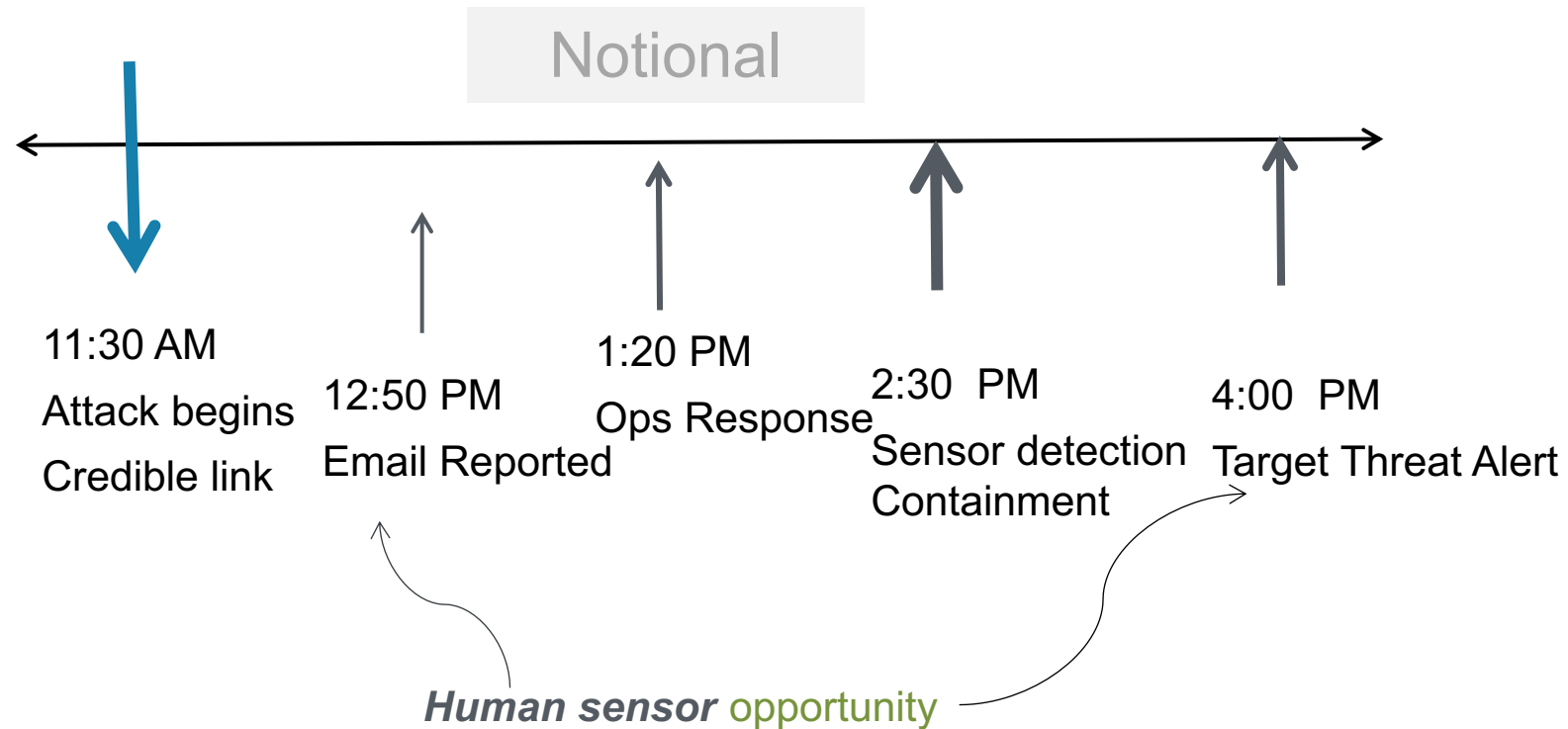
The advanced cyber adversary needs only one click with “right” conditions.

Gap Analysis



TIP: Use a spreadsheet to jump start analysis

Postmortem Gap Analysis with Human Sensors



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





Bang!

Gap analysis

Ask your cyber operations team

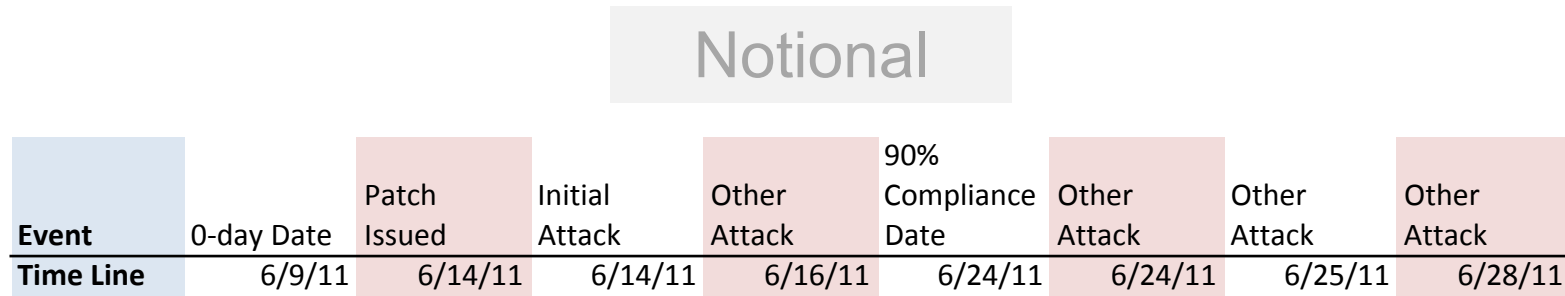
- What gets through?
- What is the scale of concern?
- Where/Who are most at-risk?

Executive action

Aha moment

- Qualify your threat landscape
- Show the means of attack
- Change the game

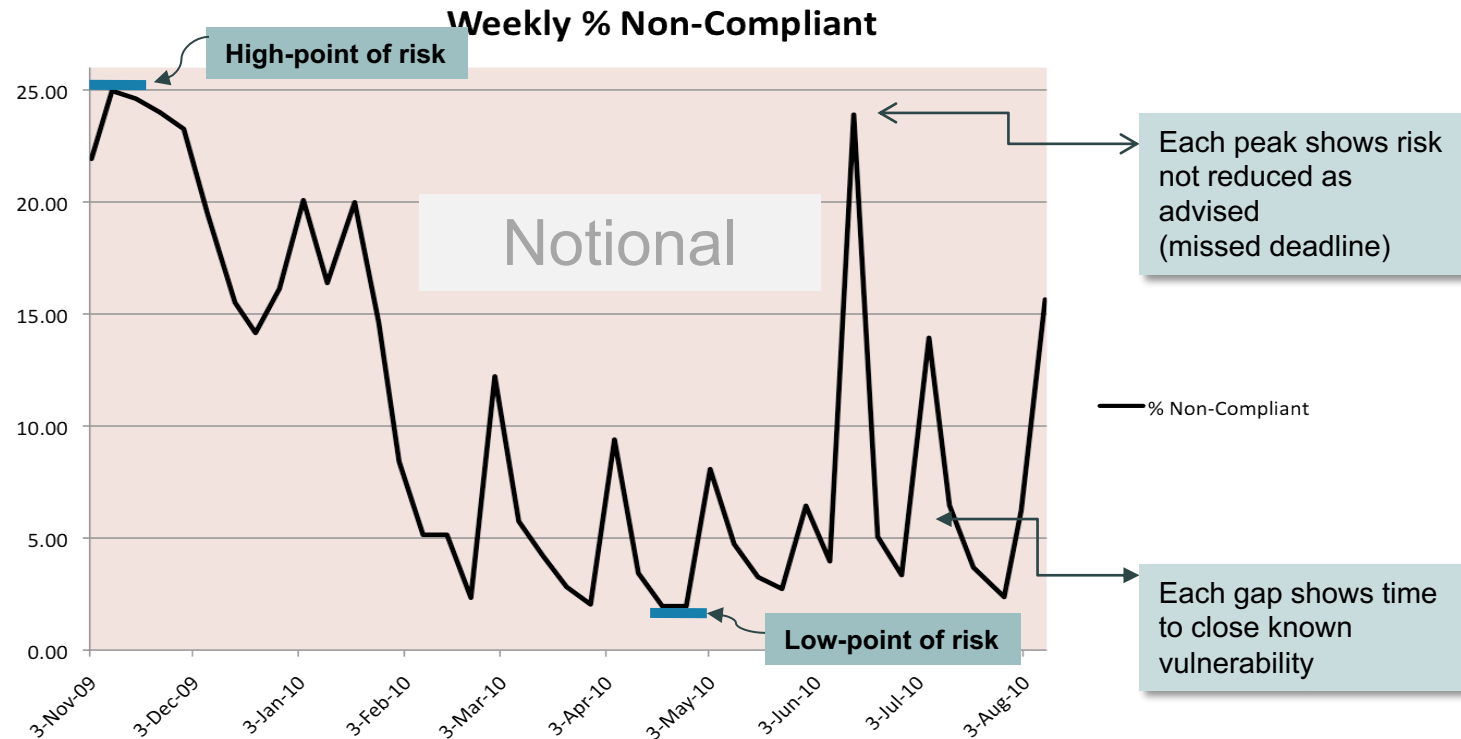
Aha Moment: Example Means of Attack



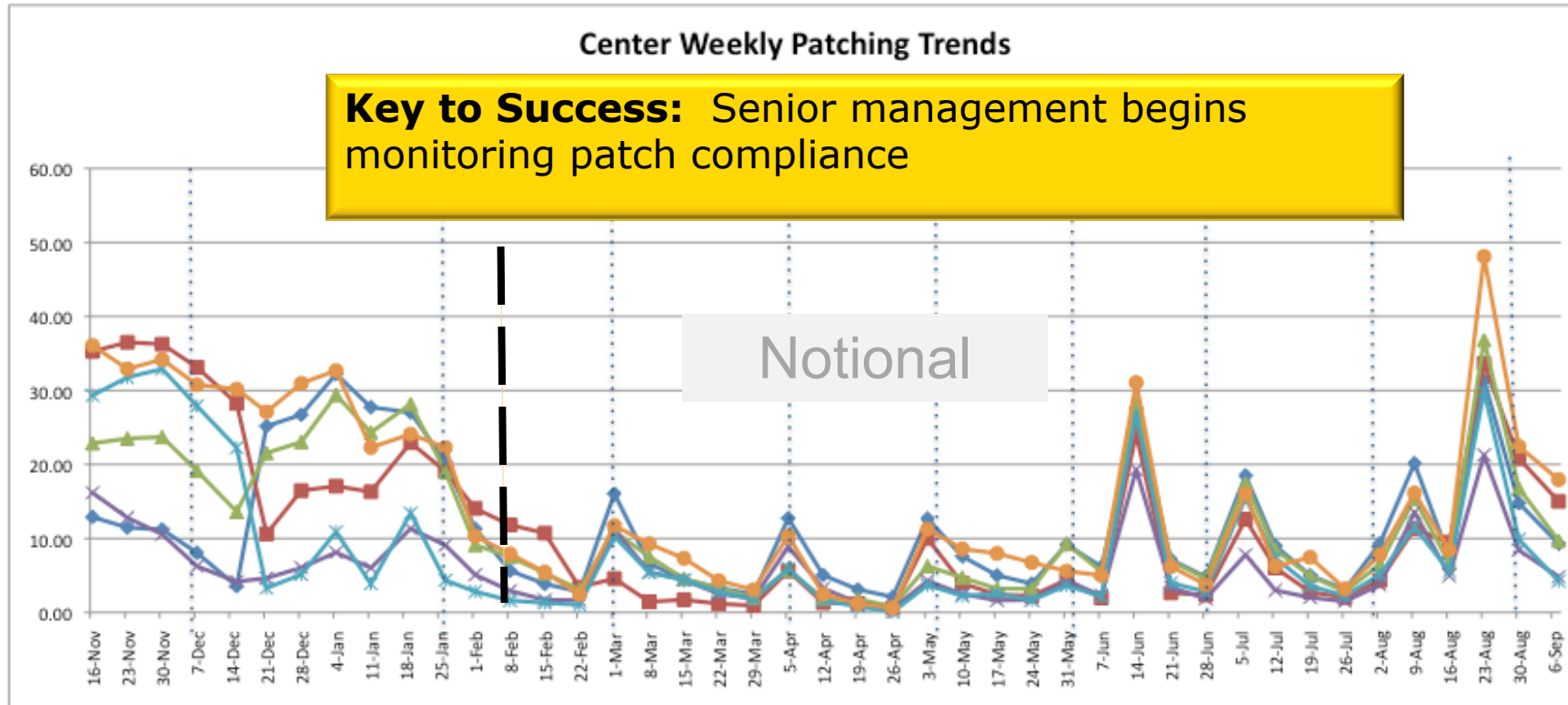
Opportunity for employees to be cyber defenders and human sensors.



Aha Moment: Example Risk Latency



Aha Moment: Executive action



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

* <http://www.infoworld.com/article/2611443/security/stop-80-percent-of-malicious-attacks-now.html>



Tell the story

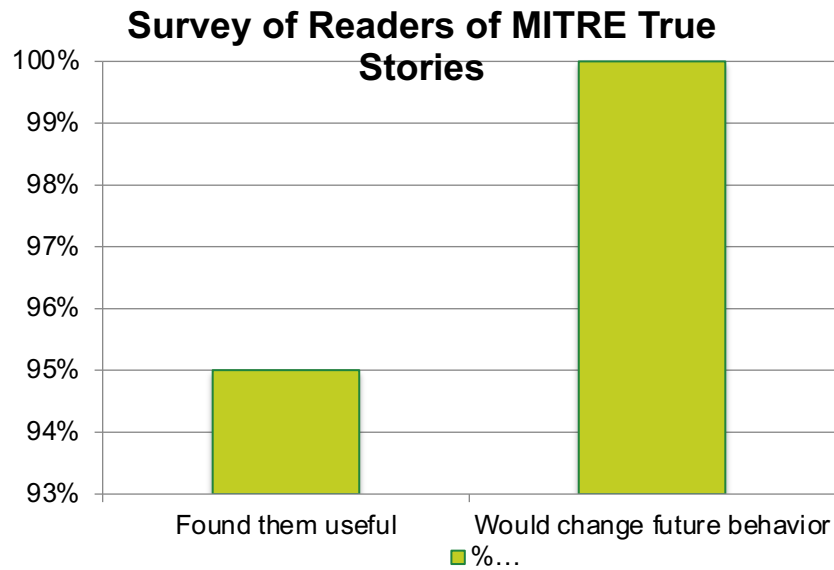
Your actual situation matters more than generalities

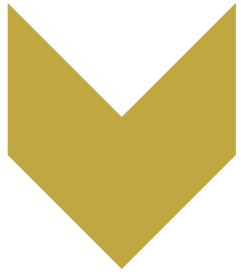
Personal stories (with people you know!) have more impact

Transparency builds trust → trust creates willingness → willingness seizes opportunity

Tell the Stories: Real Incidents

Social comparison as a basis for heightening threat awareness





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.

#	Your answer	Correct answer	Result	Reason
1	Fake	Fake	✓	Why?
2	Legitimate	Fake	✗	Why?
3	Don't know	Legitimate	✗	Why?
4	Fake	Fake	✓	Why?
5	Legitimate	Legitimate	✓	Why?
6	Legitimate	Legitimate	✓	Why?

Question 2

Callouts:

- "This appears to come from yourself, although the name says Microsoft Team."
- "Conflicker has the letter L when it should say Conficker, no L, the official name of the worm."
- "An outbreak on MITRE's network would not be communicated by Microsoft or any other vendor."
- "Microsoft would not send you a file to install, but would instead point you to their online resources."

THIS WEEK'S POLL

us Email Poll of the Week

Would you open this?

Image to open full-size in new window

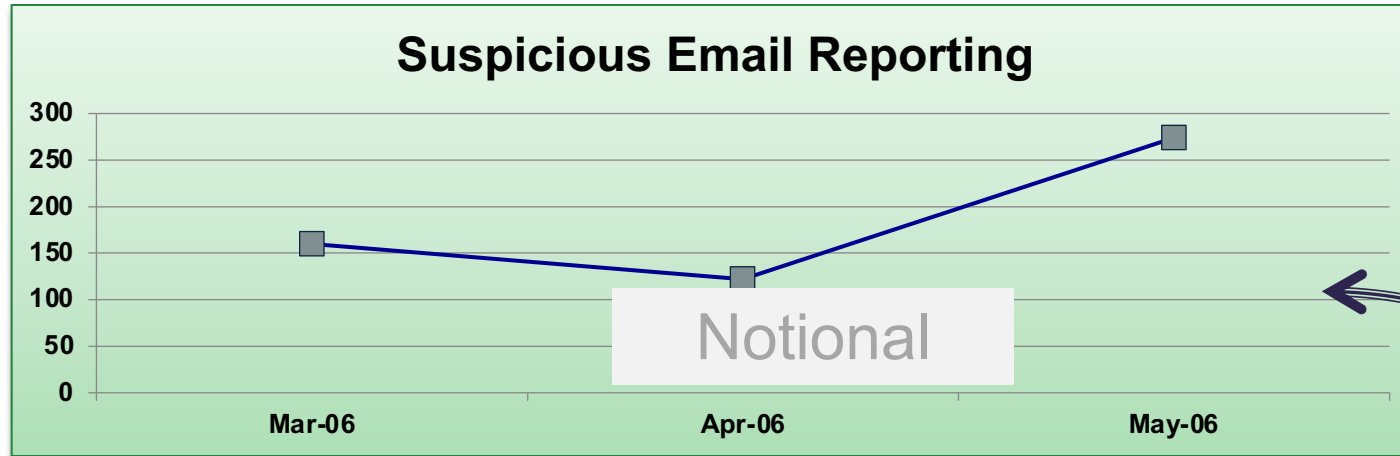
[More information...](#)

Fake	<div style="width: 45%;"></div>	45% (5)
Legitimate	<div style="width: 45%;"></div>	45% (5)
Don't Know	<div style="width: 9%;"></div>	9% (1)

Total votes: 11



Opportunity: Learn, Report, Detect



Practice “quiz” ends

Human Sensor Network: number of APT emails “discovered”

Before safe practice: 1

After safe practice: 5

Notional

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

Discussion with Reporter

reported: 2014-06-06 06:55

Thought I might forward this one. I didn't open it, but it did show in my Outlook Preview.

The reason for suspicious... I don't use my MITRE email on any external sites like LinkedIn.. I use my personal Gmail address.
Also.. the send addresses me by my last name, not first..

Thanks..
Bob

responded: 2014-06-06 07:24

Bob,

Thank you for alerting us -- reporting suspicious contacts and emails to re.org helps not only our cyber defense and cyber intelligence activities but also our counter intelligence activities.

This is likely a spoofed identity reaching out to you on LinkedIn because of your association with MITRE.

We appreciate your security sense and helping us protect MITRE.

We will send you separately a Cyber Threat Education Bulletin to help you secure your account and reduce your risk.

Best regards,

MITRE InfoSec Cyber Threat Awareness

Respond: Focused Alerting

Cyber Threat Alerts

Delivered and intercepted attacks

Pre-attack warnings to known targets

Phishing alerts

All Employee Alert Posted



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 J [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](mailto: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



Invitation to a MITRE InfoSec Threat Briefing

Why Am I Invited?

MITRE InfoSec has received information that indicates that you and/or your project are a potential target of phishing emails and malware infested attachments.

To enable you to protect your systems and information, we ask that you attend the Threat Awareness briefing described in this invitation.

MILCOM Organizers

As an organizer of the upcoming MILCOM 2009 event, your name and email address have been exposed on the Internet. As a result, you will likely become the recipient of seemingly valid email messages that may instead contain malware or lures to malicious web sites.

Threat Awareness and Readiness

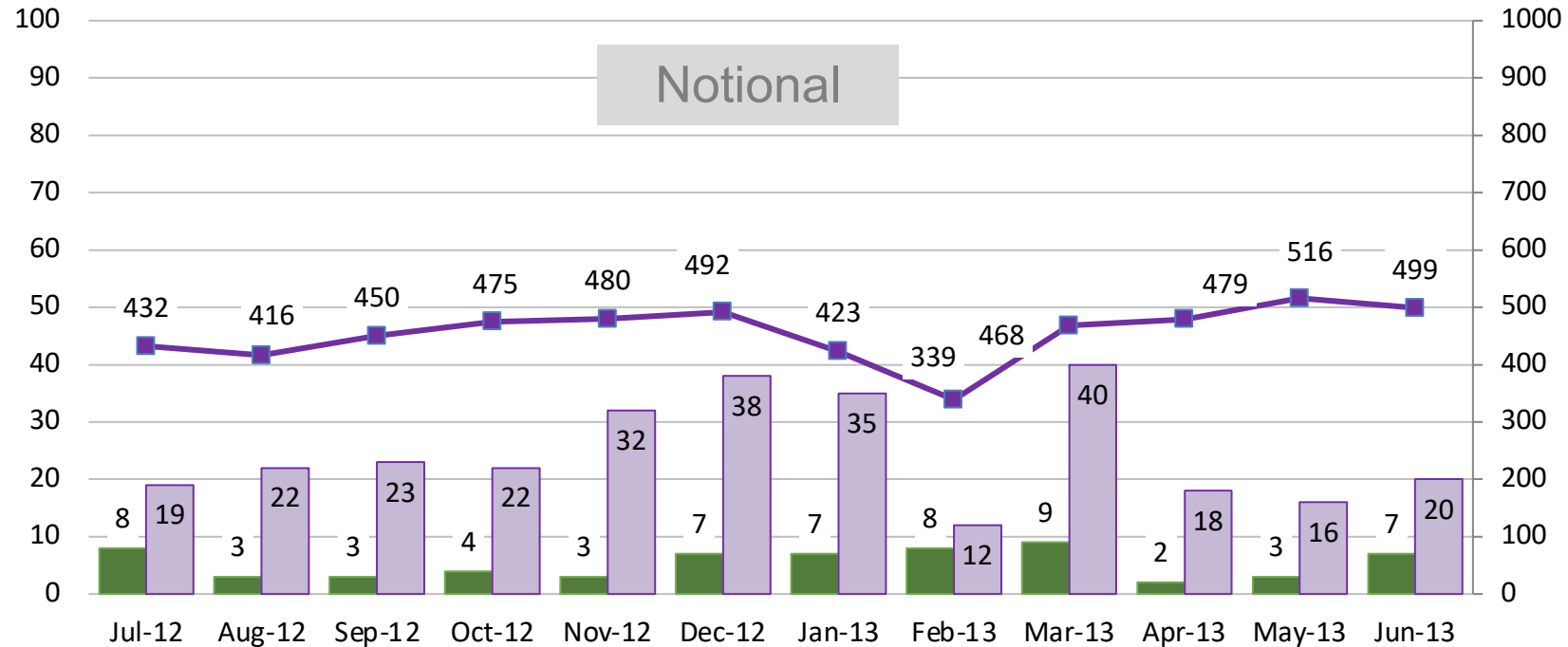
MITRE InfoSec would like to brief you on the threats specific to you as an organizer of the MILCOM 2009 event. This will enable you, as well as us, to better protect MITRE and its information.

You will be receiving a Meeting Invitation. Should you need to contact us regarding this invitation, please call , or

 **MITRE InfoSec**
Assuring System and Information Security

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 for Malware Analysis
- Number of Suspicious Email Reports

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 with headers
Importance: High text/plain 1.3KIB

You help is need.

Yesterday (Monday, Jul [redacted]) 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.

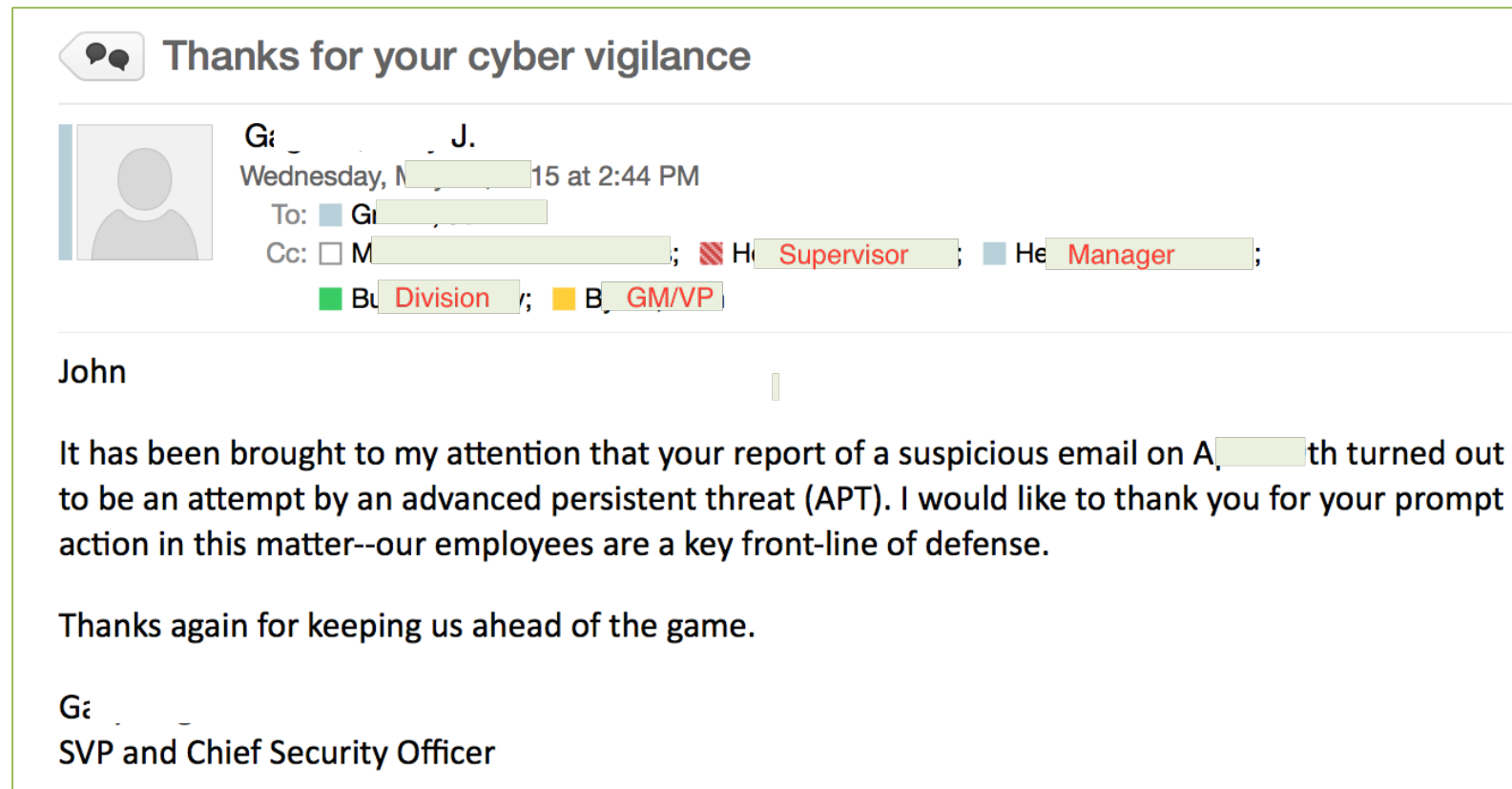
We rely on you for MITRE's cyber defense, so please report any odd messages to sus [redacted] org and any clicks that you regret or that do not do what you expect – doing so can help us stop a cyber attack. Please don't assume that any defense or sensor will detect or protect MITRE from the cyber adversary.

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



TAKE-AWAY Personalization, appreciation, and recognition motivate willingness to report.

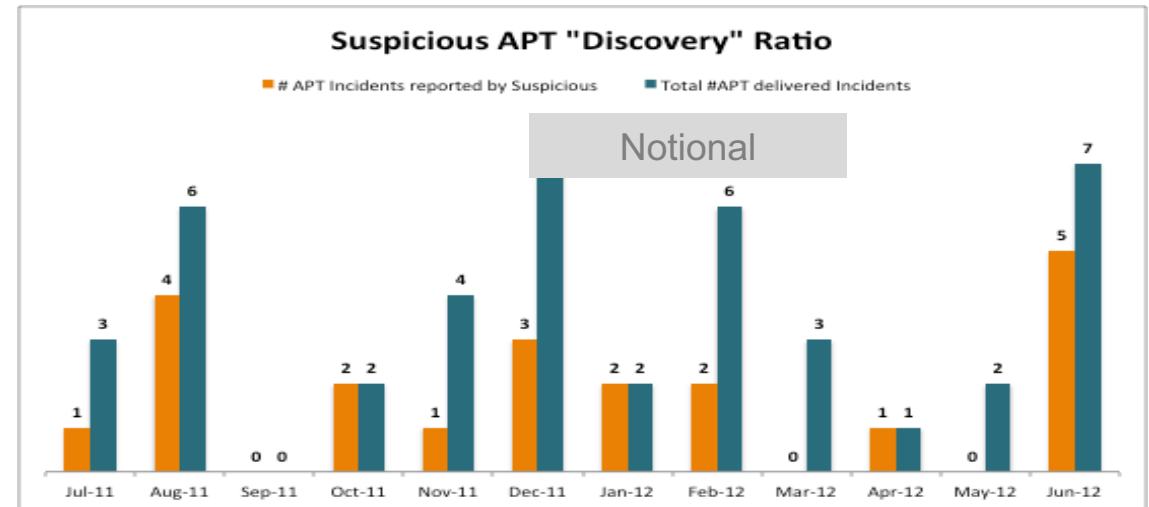
Human Sensor Evolution

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

Operational Best Practices for Suspicious Email

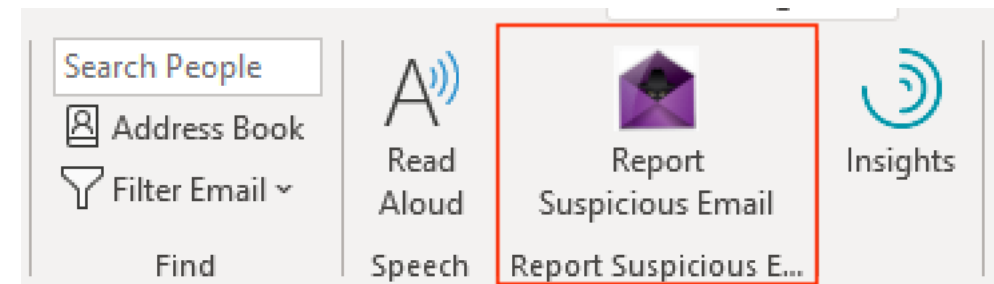
Apply a banner or tag to inbound email

Colored warning banners in the body or a tag, such as [EXT], in the subject line, gives staff visual indicators for external email handling



Report Suspicious Email button

Make user reporting easier and ready for analysis by incorporating a button in the email client that sends the suspect email with mail headers



Outlook ribbon

Ellen Powers

ejpowers@mitre.org

 **[@MITREcorp](https://twitter.com/MITREcorp)**

 **[linkedin.com/company/mitre](https://www.linkedin.com/company/mitre)**