How to Establish a Suspicious Email Program and Educate End Users

Ellen Powers

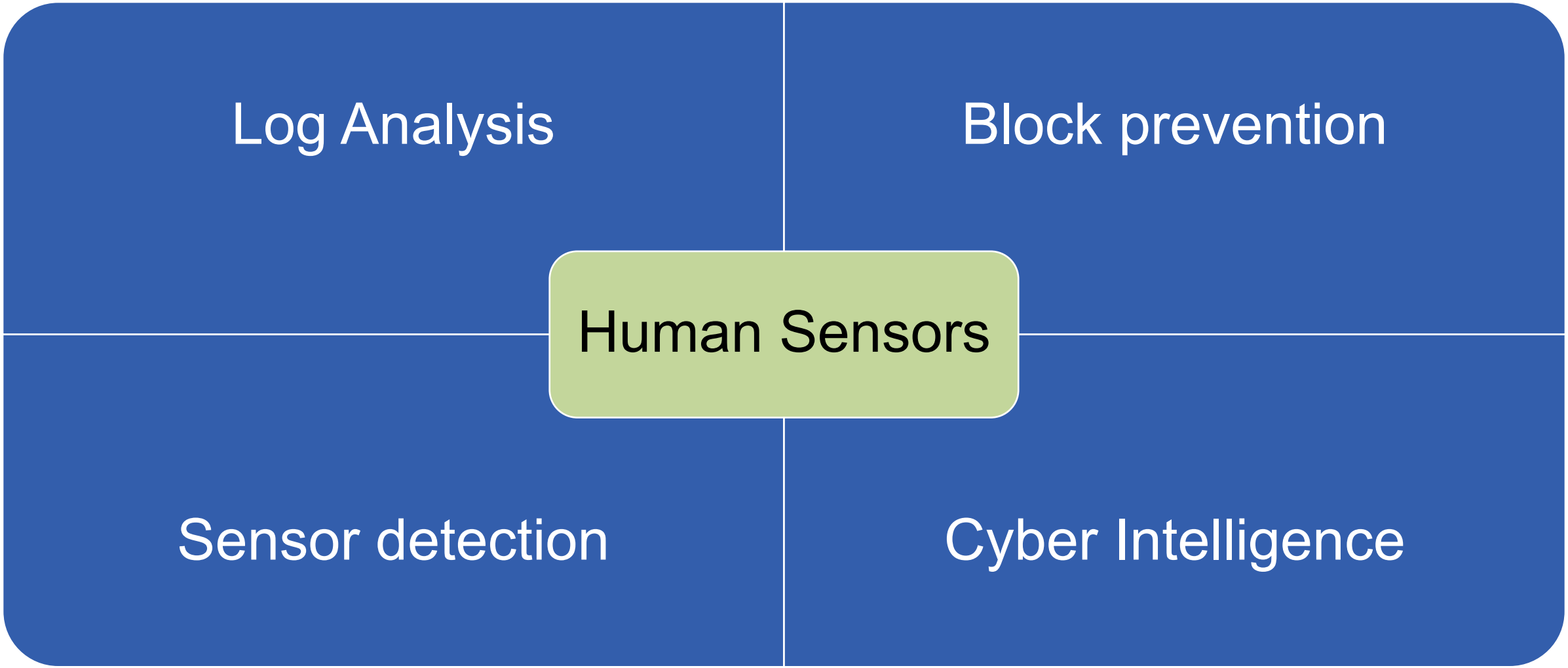
January 2021

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

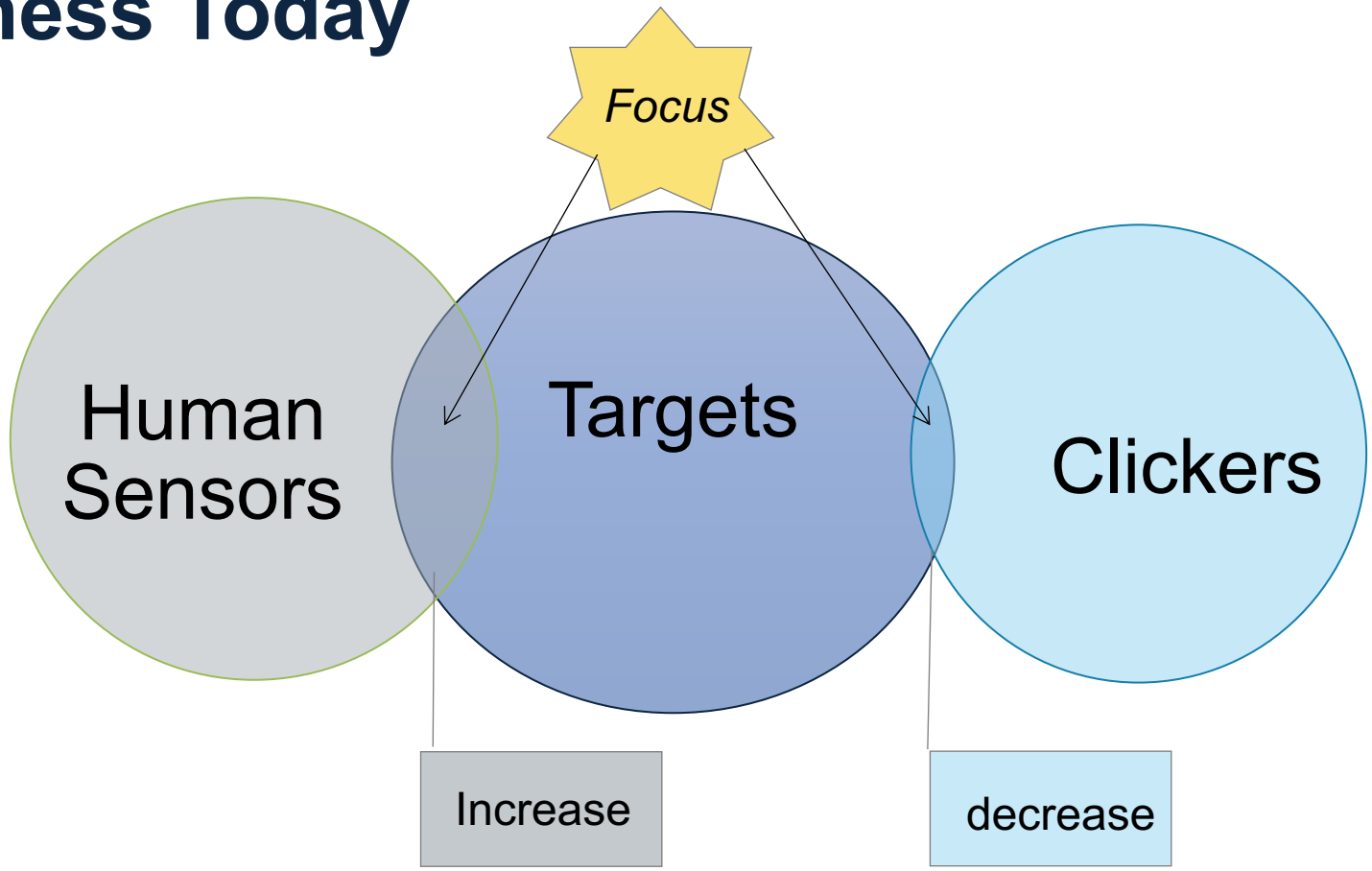
Suspicious Email Program Goal

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

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?

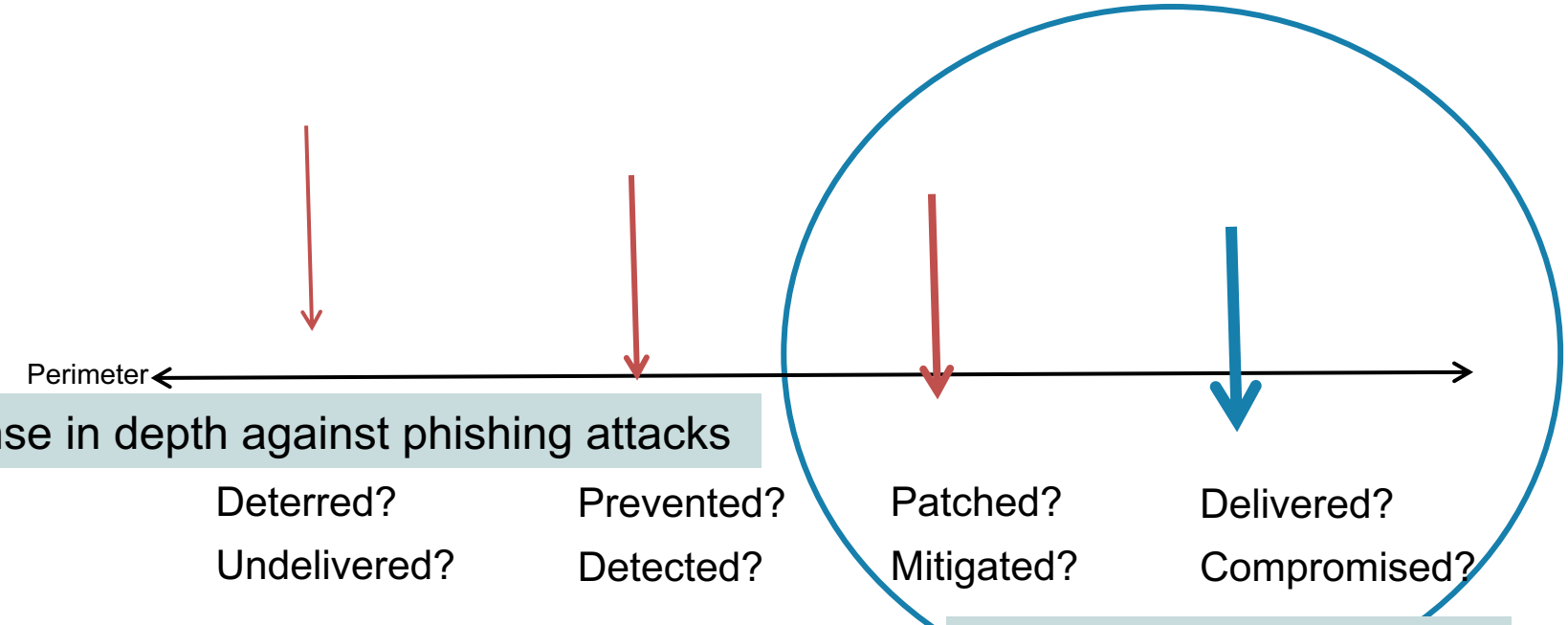
Cyber Threat Landscape Highlight

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



Defense in depth against phishing attacks

Deterred?
Undelivered?

Prevented?
Detected?

Patched?
Mitigated?

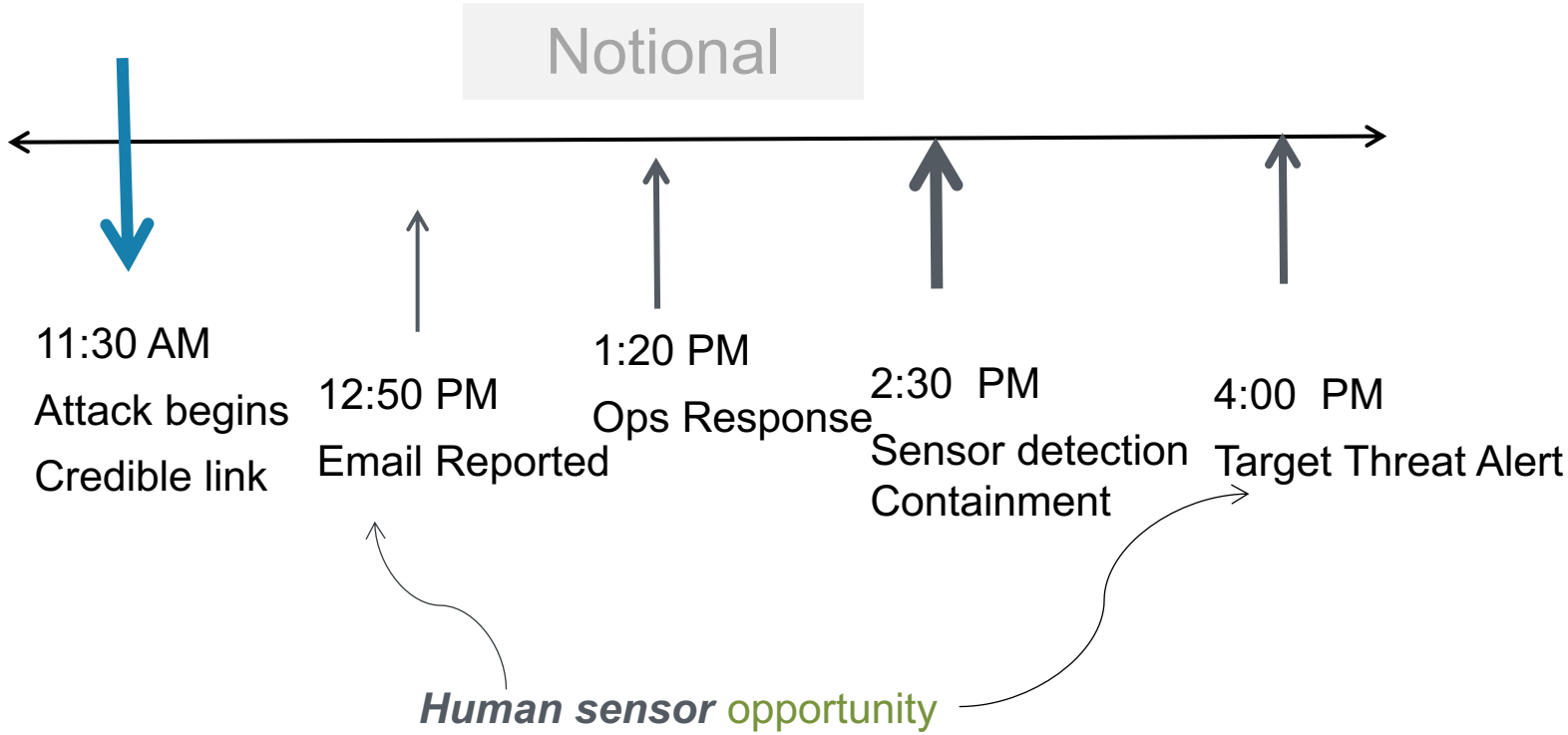
Delivered?
Compromised?

Analyze what got through

- Subjects/themes?
- Links/attachments?
- New target/known target?
- Reporter? Clicker?
- Threat actor groupings?

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.

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

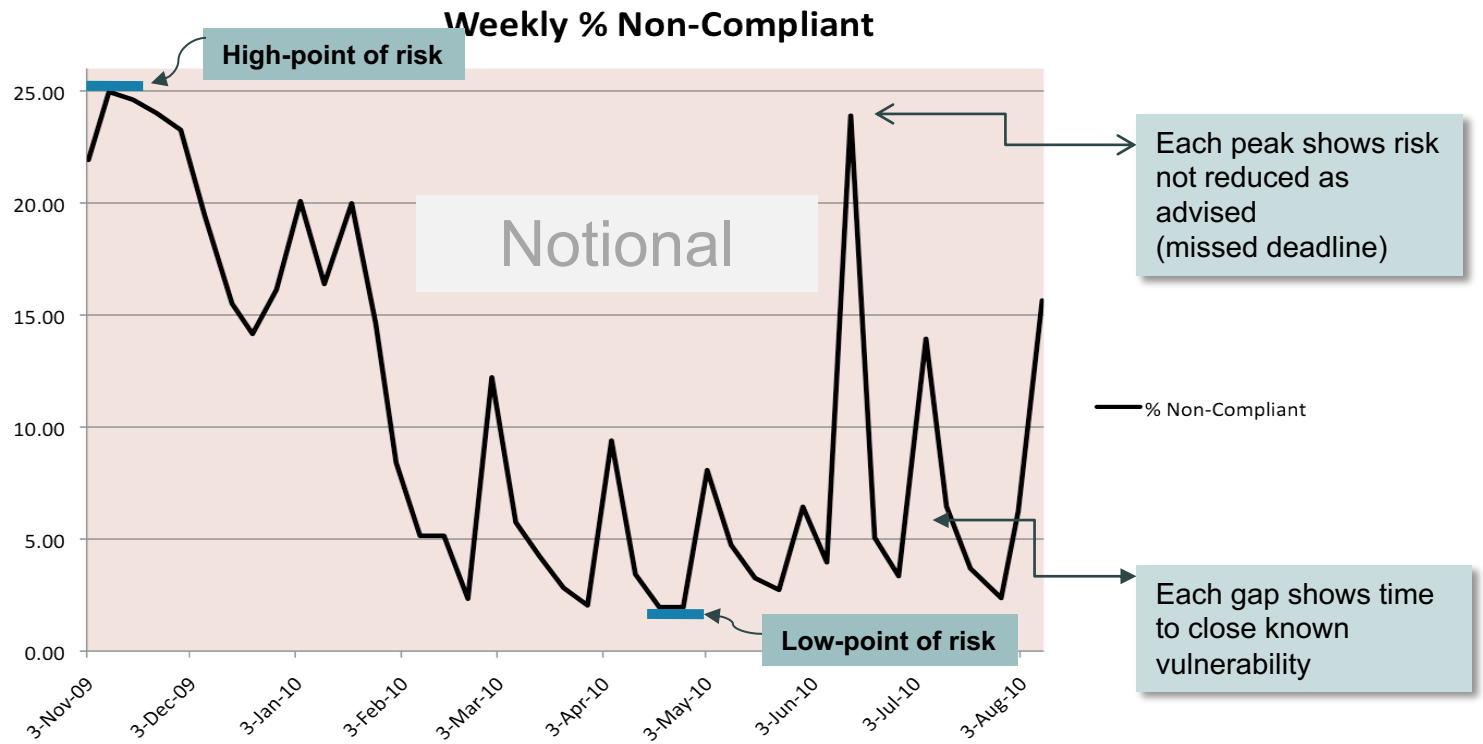
Notional

Event	0-day Date	Patch Issued	Initial Attack	Other Attack	90% Compliance Date	Other Attack	Other Attack	Other Attack
Time Line	6/9/11	6/14/11	6/14/11	6/16/11	6/24/11	6/24/11	6/25/11	6/28/11

Opportunity for employees to be cyber defenders and human sensors.

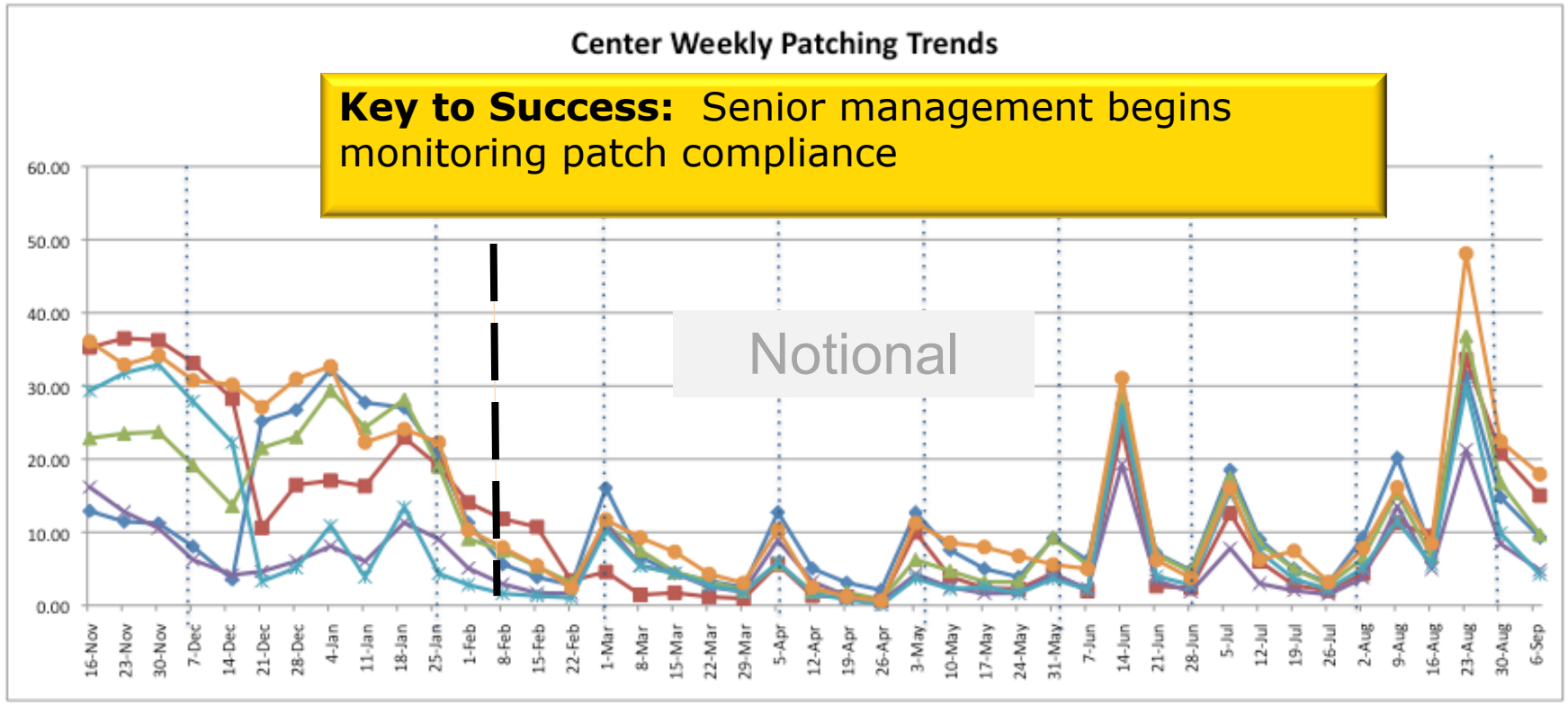
Measure!

Aha Moment: Example Risk Latency



Measure!

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

Ready

Tell the story

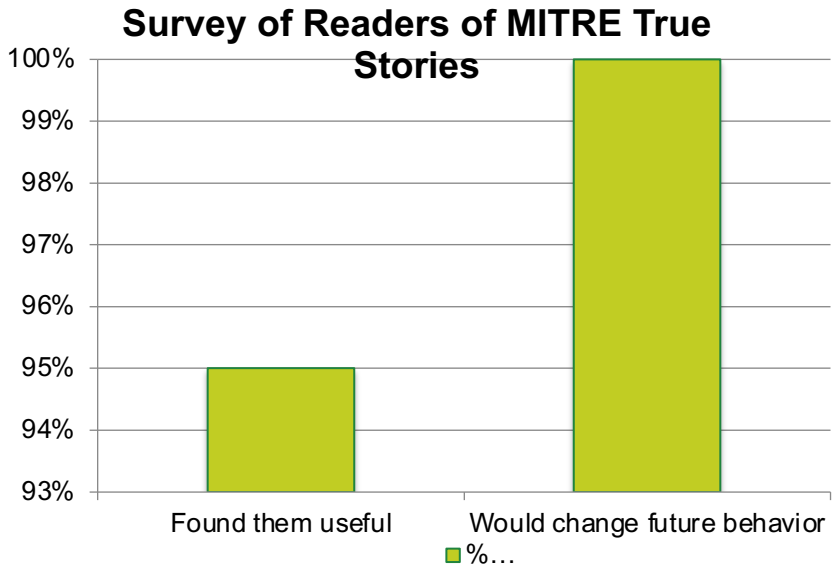
Your actual situation matters more than generalities

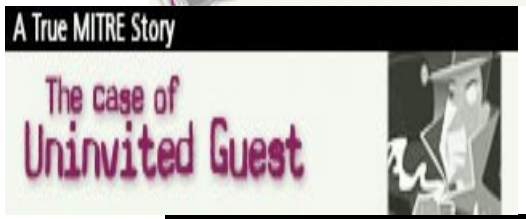
Personal stories (with people you know!) have more impact

Transparency builds trust → trust creates willingness → willingness seizes opportunity

Tell the Stories: Real Incidents

Social comparison as a basis for heightening threat awareness





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

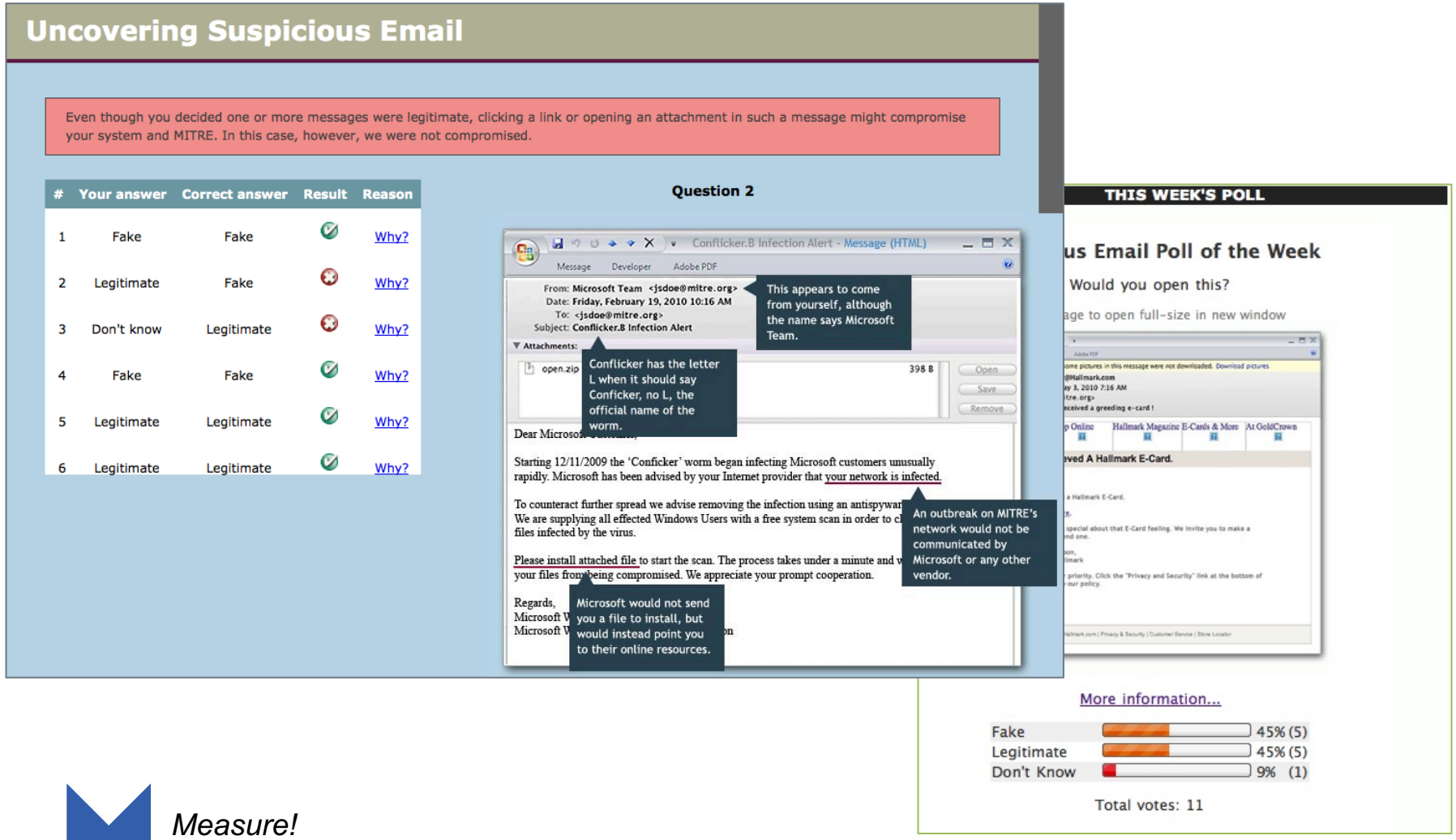
Starter Method
Email Self-questioning Technique

- Expected?
- Ambiguous?
- Relationship?
- Normal?
- Exposed?
- Sense?
- Time?

Active Uncertainty Method
Email SOS

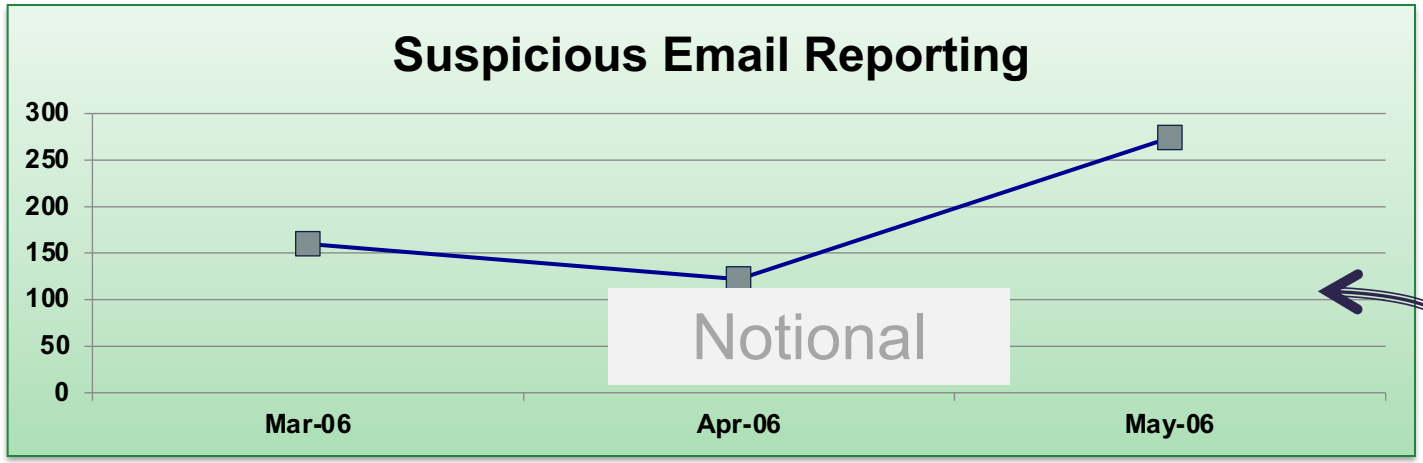
- Check Sender address and name
- Hover Over the links
- Determine if the messages makes Sense

Opportunity: Safe Practice



Measure!

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

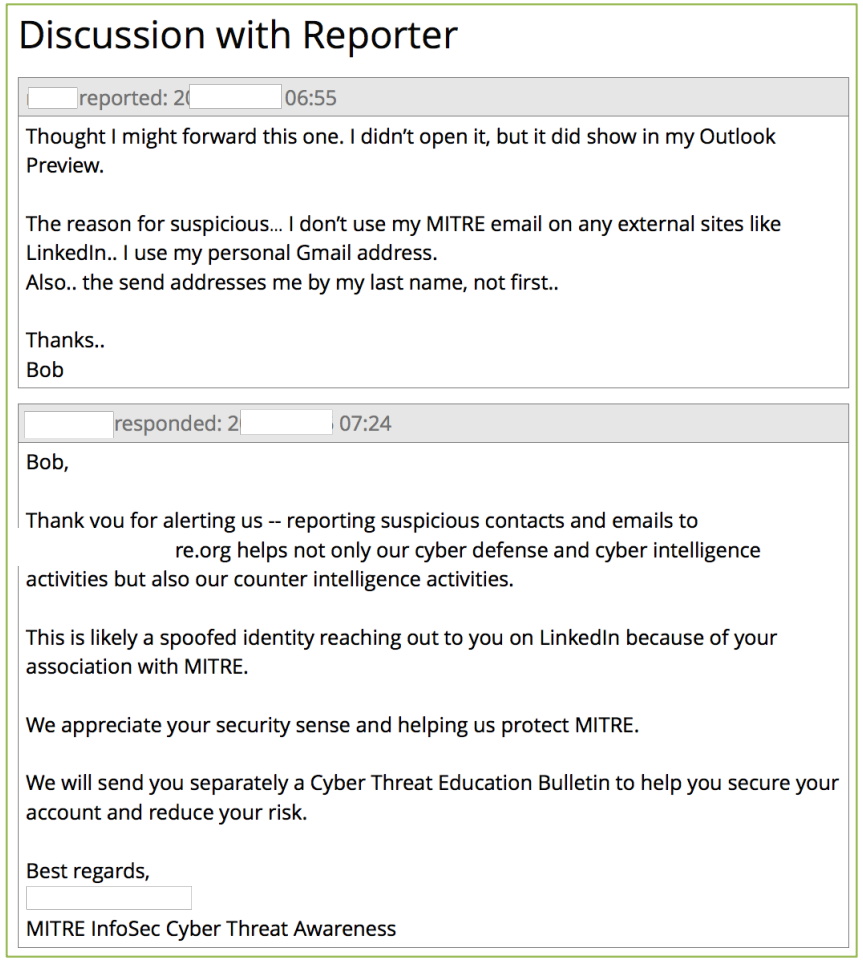
Personalized responses

Learning opportunity

Threat Awareness

Enable self-reporting

Acknowledgement and appreciation rather than penalty



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 — sometimes a **user report** is the only **alert** we receive.

We appreciate your help defending your inbox and MITRE.

Best regards,

[redacted]

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

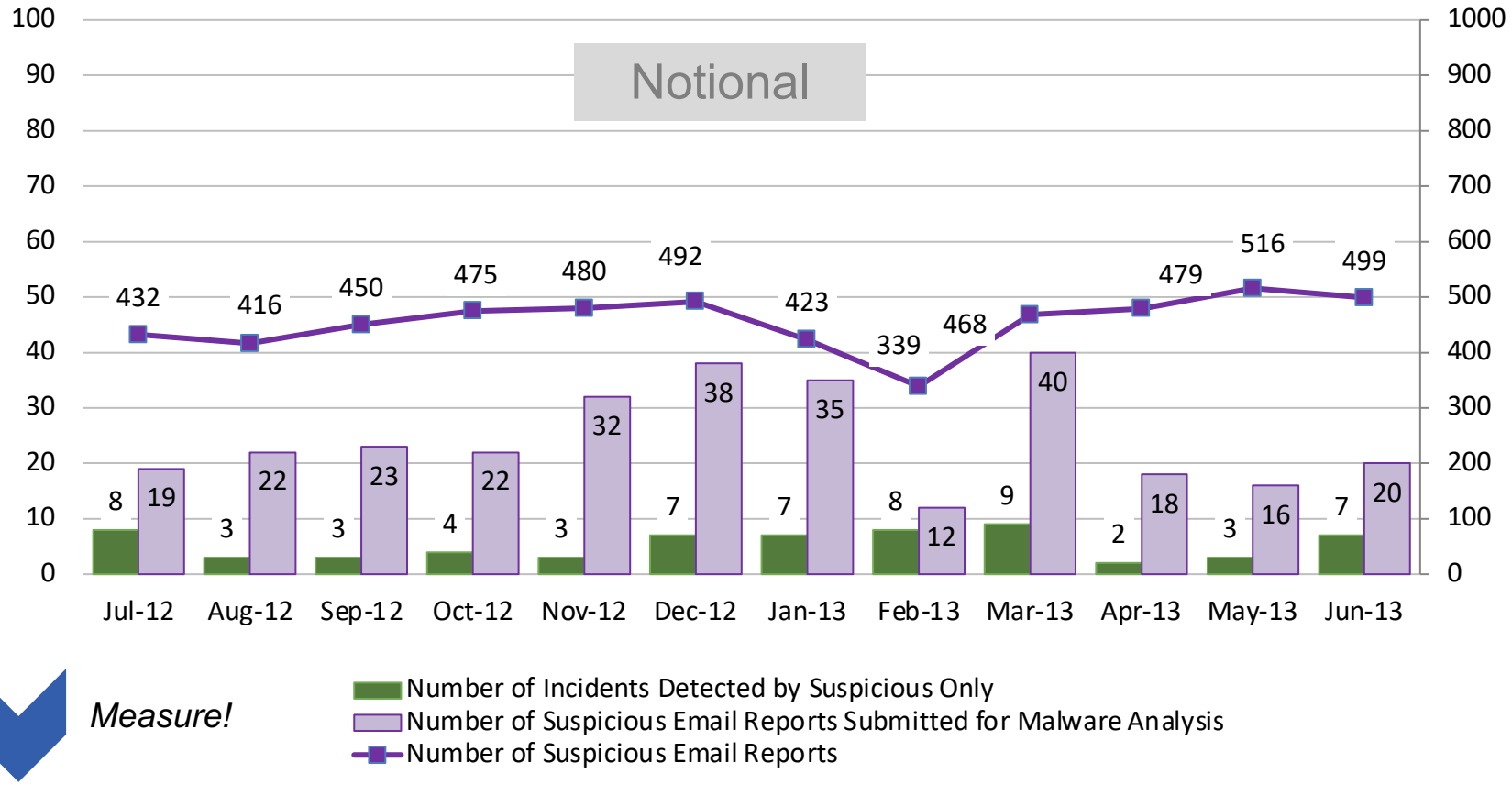
What to look for

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



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

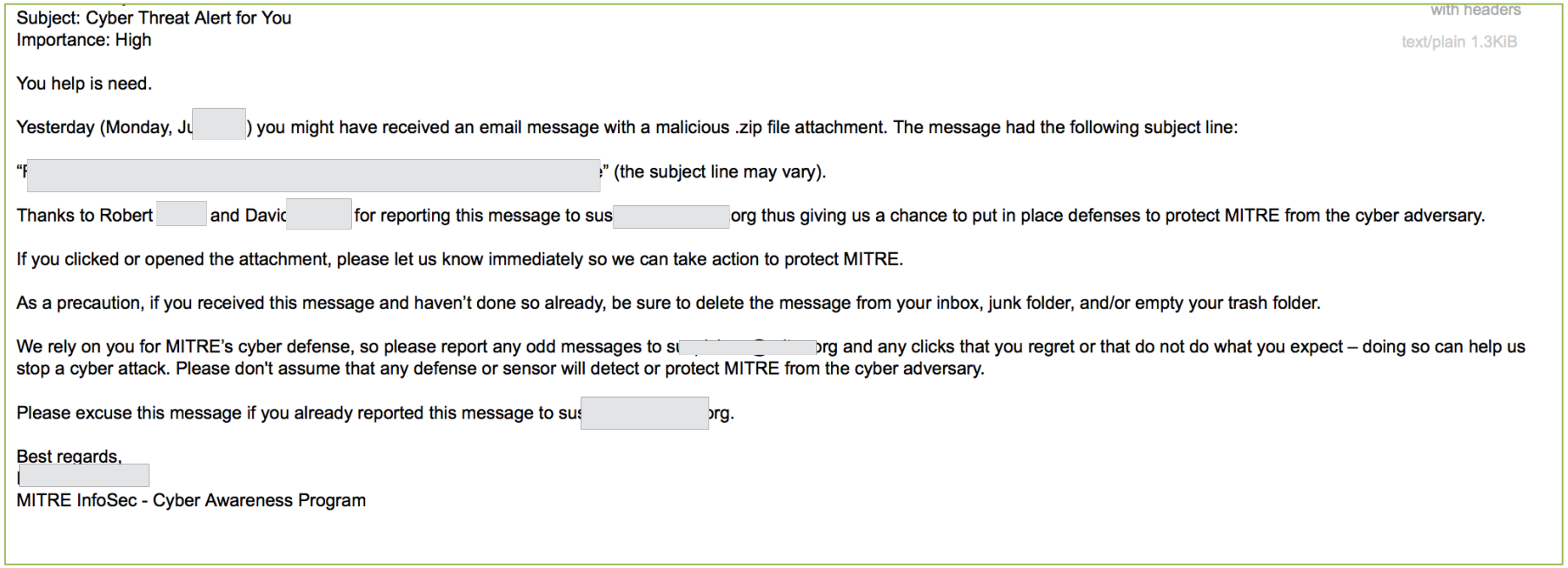
C-level kudos

Recognize: Shout-outs

Phishing alerts acknowledge those who have reported

Shared responsibility for cyber defense

Shows how employee reporting makes a difference



with headers

text/plain 1.3KiB

Subject: Cyber Threat Alert for You
Importance: High

You help is need.

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

“ ” (the subject line may vary).

Thanks to Robert and Davi for reporting this message to sus 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.

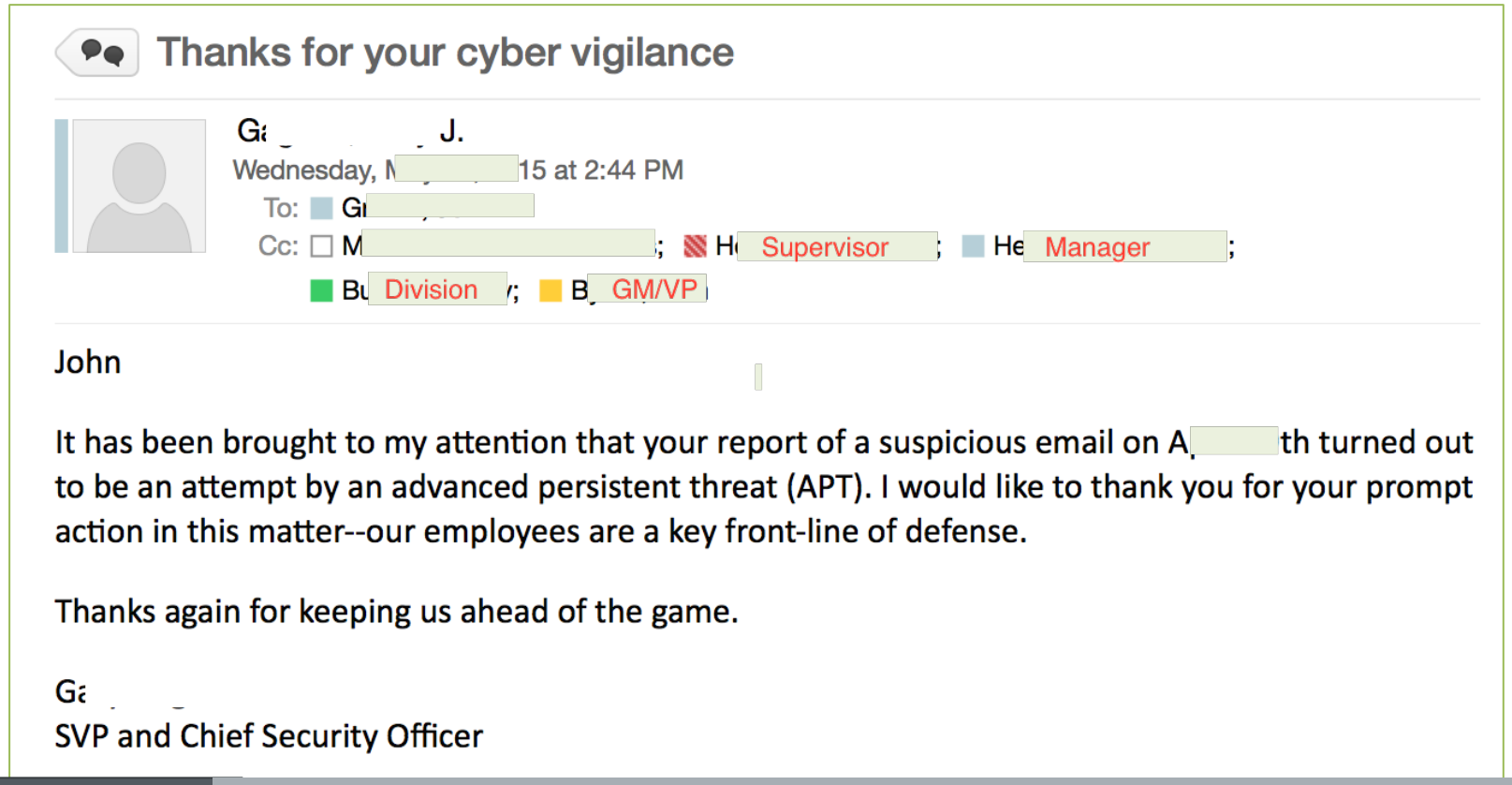
We rely on you for MITRE’s cyber defense, so please report any odd messages to s rg and any clicks that you regret or that do not do what you expect – doing so can help us stop a cyber attack. Please don't assume that any defense or sensor will detect or protect MITRE from the cyber adversary.

Please excuse this message if you already reported this message to sus rg.

Best regards,
MITRE InfoSec - Cyber Awareness Program

Recognize: Kudos for Human Sensor

CSO recognizes individuals who report advanced threat email



Thanks for your cyber vigilance

Ga J.

Wednesday, M 15 at 2:44 PM

To: Gi

Cc: M; H Supervisor; He Manager;

Bu Division; B 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.

Ga

SVP and Chief Security Officer

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

Human Sensor Evolution

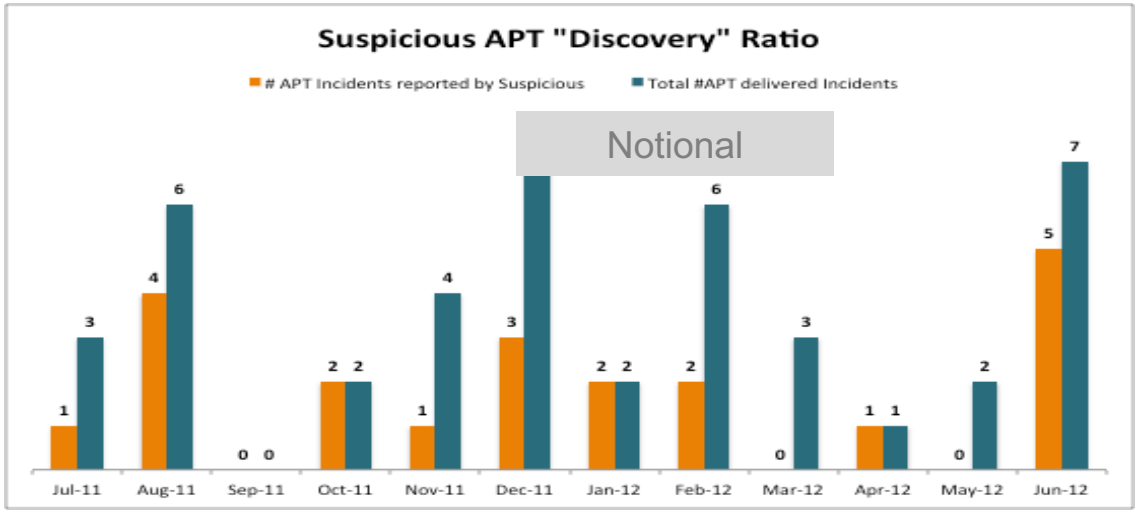
Delivered advanced threats

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

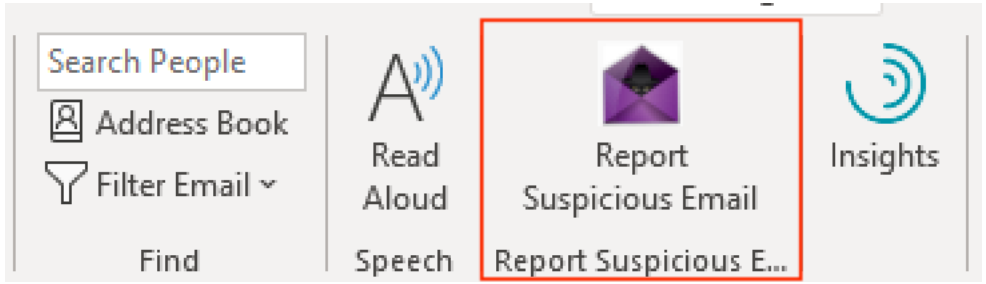
Operational Best Practices for Suspicious Email

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

linkedin.com/company/mitre

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™