CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION TECHNOLOGY

CMS Data Guardian Program

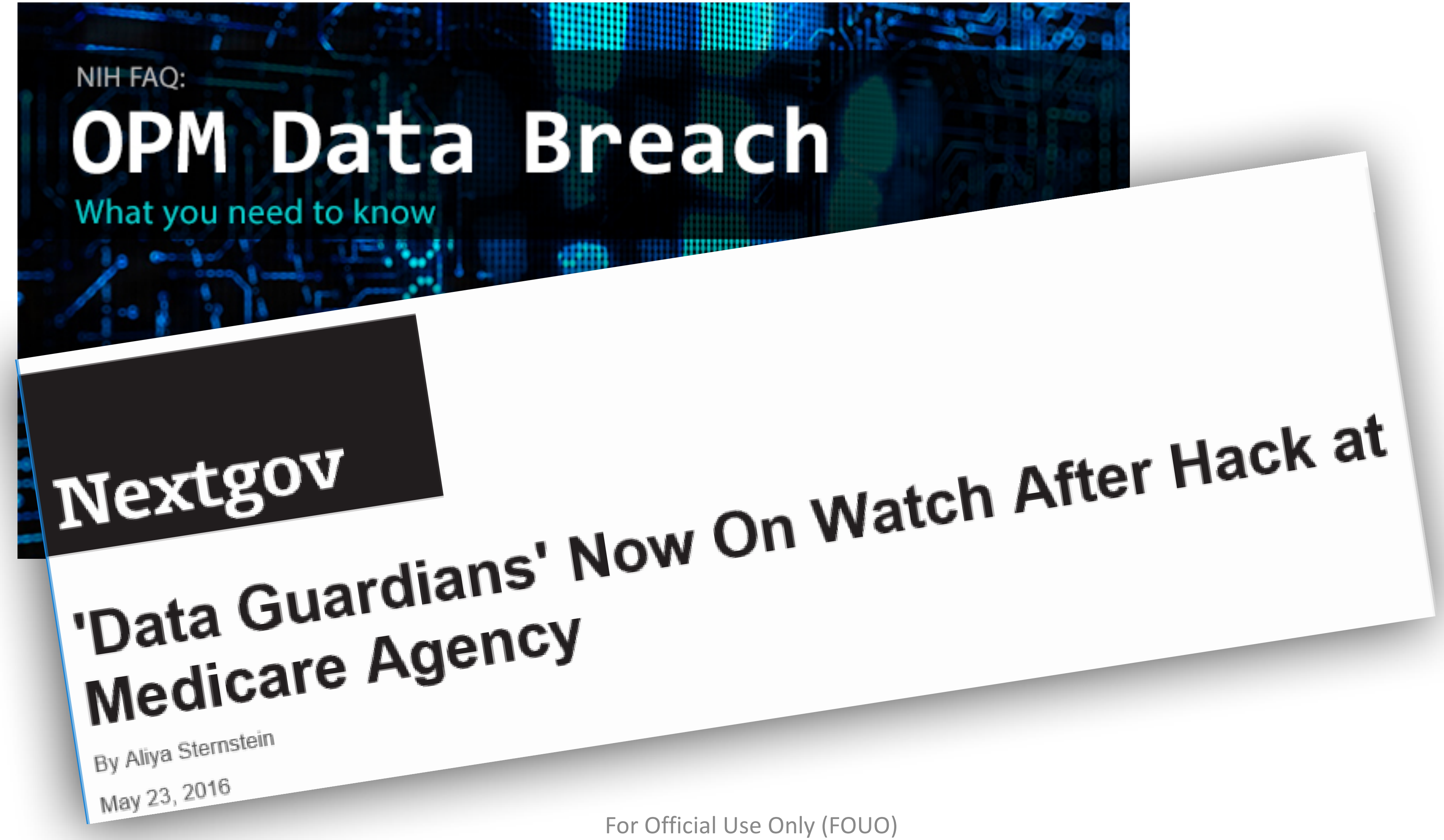
NIST FISSEA Conference

March 14, 2017

Karen Mandelbaum, Director,
Division of Security, Privacy Policy & Governance

Micah Batchelder, Federal Lead,
Incident Management Team

Introduction



NIH FAQ:

OPM Data Breach

What you need to know

Nextgov

'Data Guardians' Now On Watch After Hack at Medicare Agency

By Aliya Sternstein

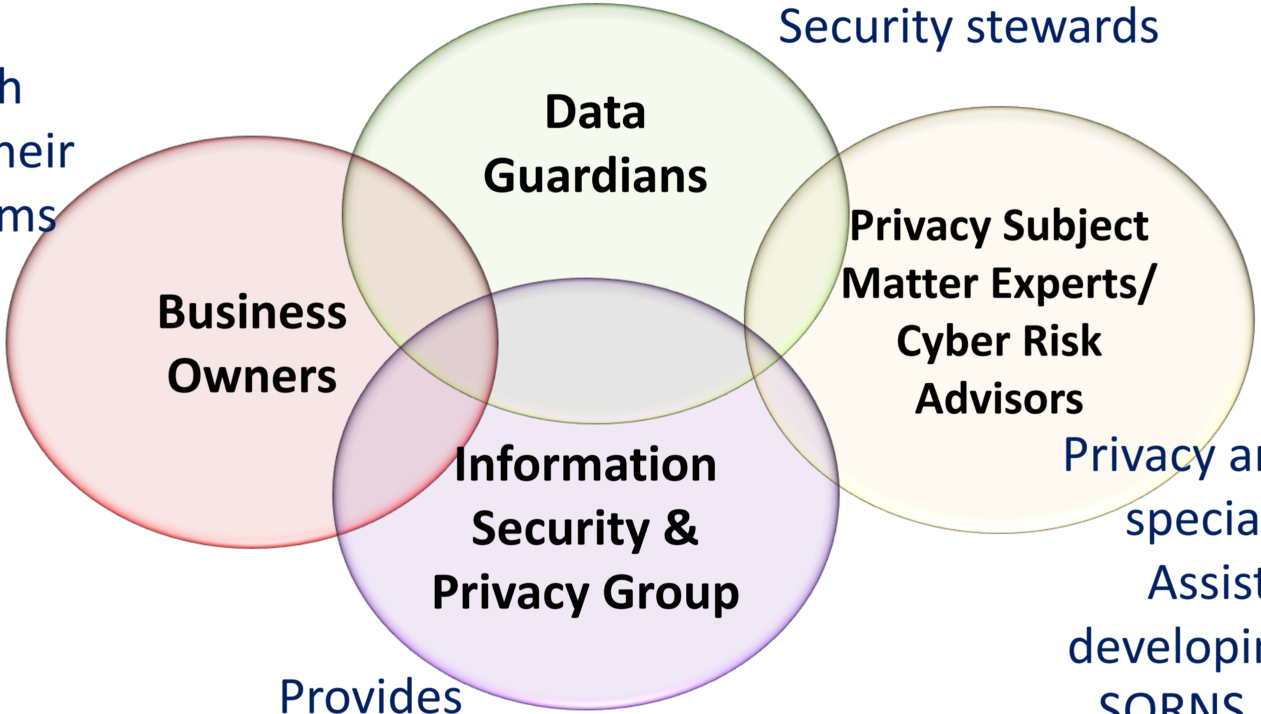
May 23, 2016

Data Guardian as Privacy Steward

https://www.dreamstime.com

Data Guardian are responsible for disseminating the message that fortifies the culture and encourages staff to *stop*, *think*, and *ask* before taking a risk that could potentially compromise the IT systems or data of the organization.

Stakeholder Dependencies


Data Guardians
Business Owners
Privacy Subject Matter Experts/ Cyber Risk Advisors
Information Security & Privacy Group

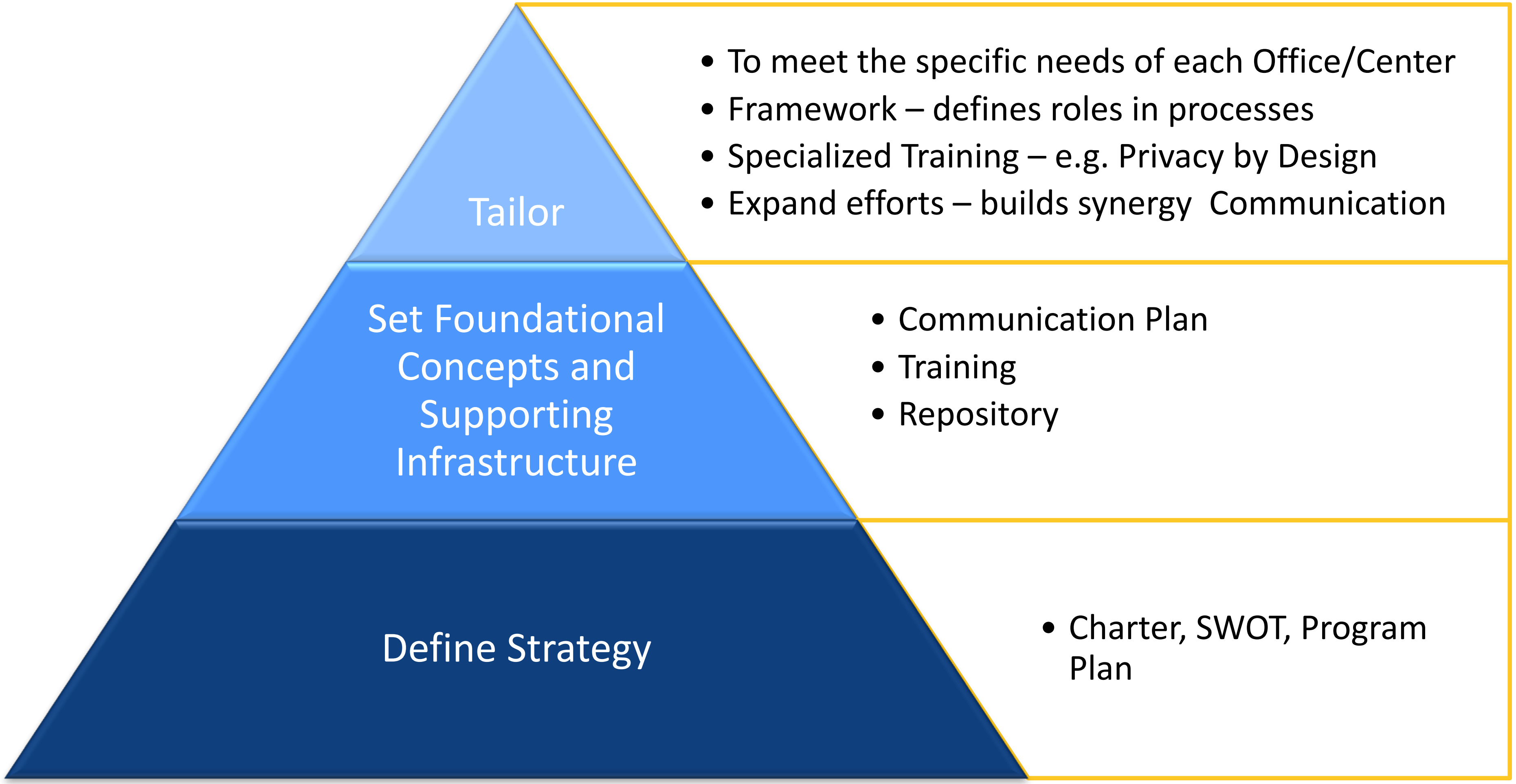
Privacy and
Security stewards

Have in-depth
knowledge of their
data and systems

Privacy and Risk
specialists
Assist in
developing PIA,
SORNS, Data
Sharing
Agreements, etc.

Provides
Training
Cyber Awareness
Briefs
Policy/Procedure

Building the Data Guardian Program



Tailor

- To meet the specific needs of each Office/Center
- Framework – defines roles in processes
- Specialized Training – e.g. Privacy by Design
- Expand efforts – builds synergy Communication

Set Foundational Concepts and Supporting Infrastructure

- Communication Plan
- Training
- Repository

Define Strategy

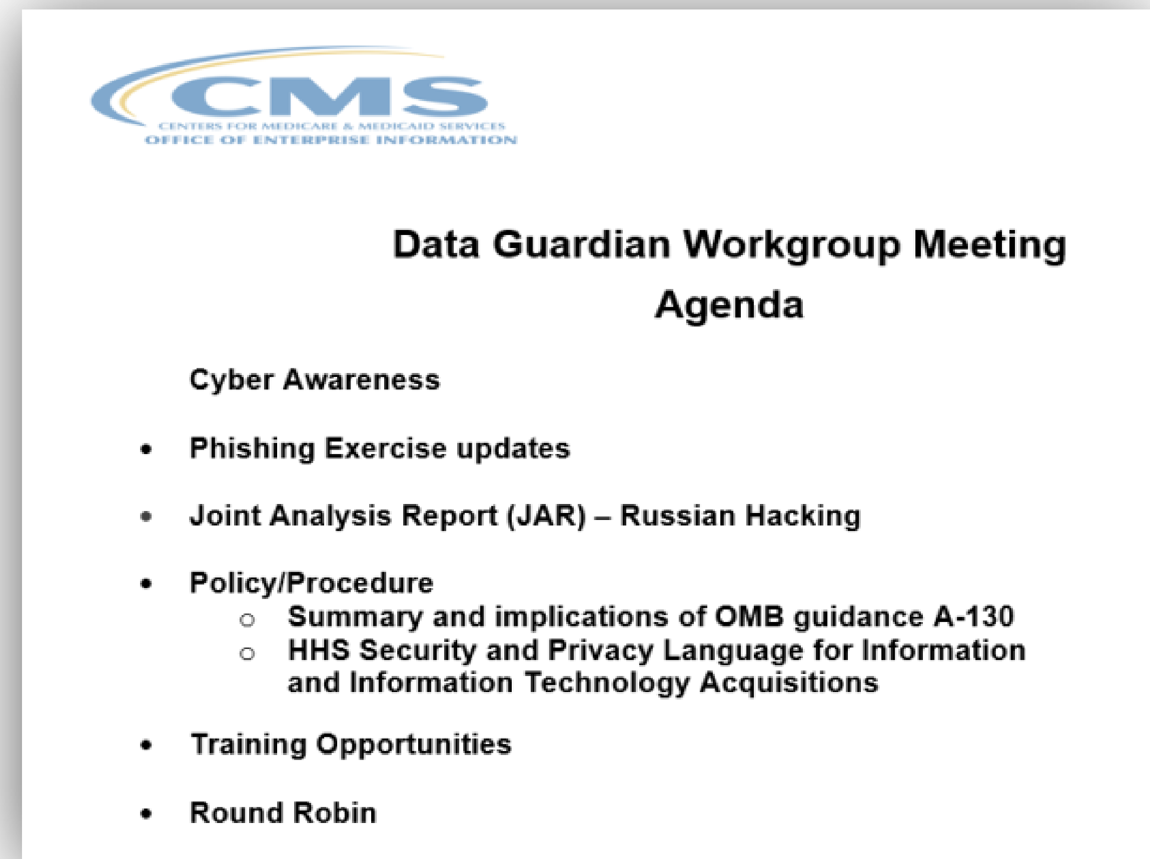
- Charter, SWOT, Program Plan

Data Guardian Meeting Agenda

What's happening internally/externally in the cyber world

&

what Data Guardians need to know and act on



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF ENTERPRISE INFORMATION

Data Guardian Workgroup Meeting Agenda

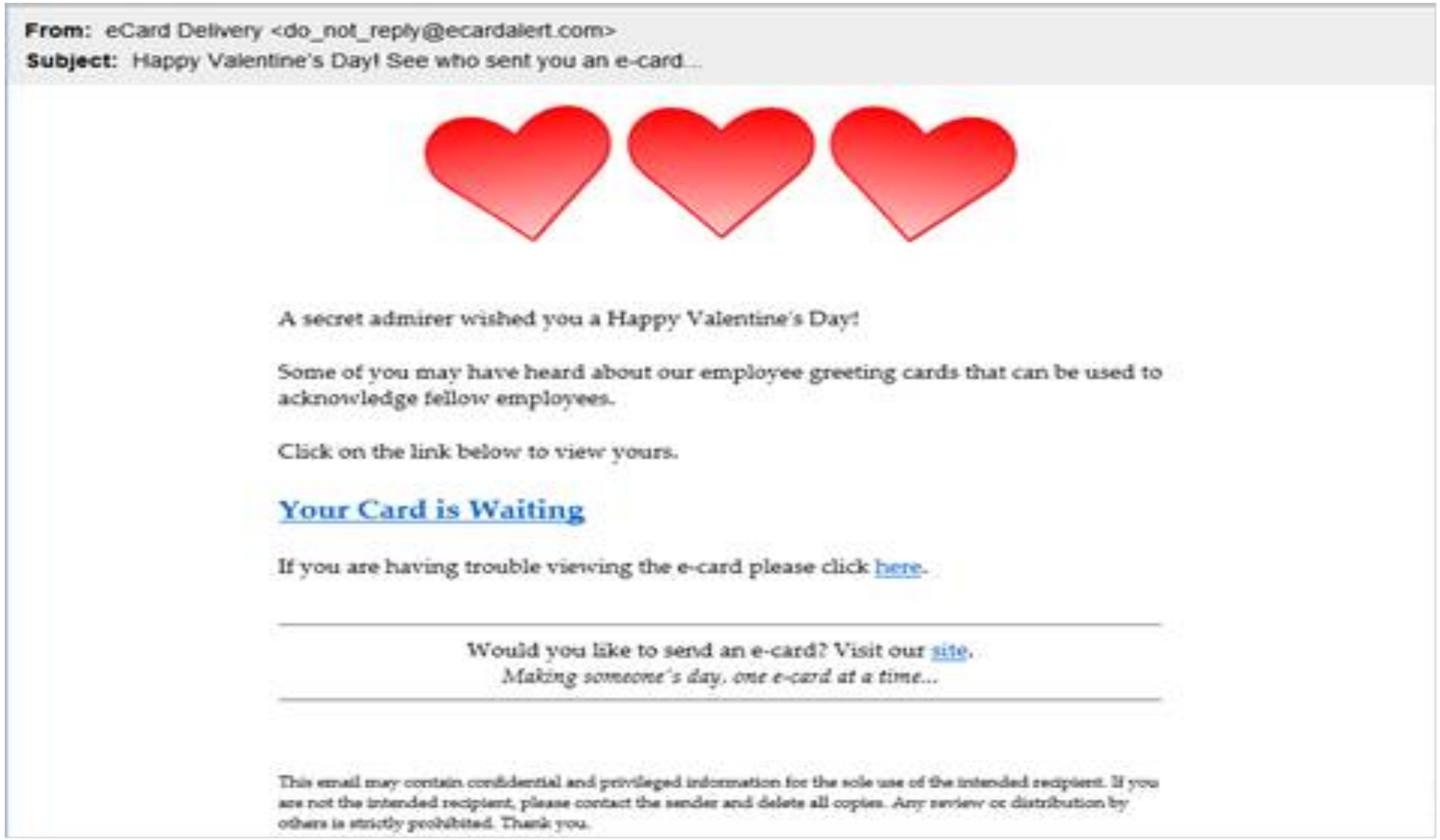
Cyber Awareness

- Phishing Exercise updates
- Joint Analysis Report (JAR) – Russian Hacking
- Policy/Procedure
  - Summary and implications of OMB guidance A-130
  - HHS Security and Privacy Language for Information and Information Technology Acquisitions
- Training Opportunities
- Round Robin

Phishing Program Overview

- Define Phishing
- Identify Phishing Scams
- Develop Scenarios and Run Exercises
- Review Statistics
- Communicate Results
- Develop Mitigation Tactics
- Compile Lessons Learned from Phishing results

Phishing Exercise Example
Valentines Day



From: eCard Delivery <do_not_reply@ecardalert.com>
Subject: Happy Valentine's Day! See who sent you an e-card...

A secret admirer wished you a Happy Valentine's Day!

Some of you may have heard about our employee greeting cards that can be used to acknowledge fellow employees.

Click on the link below to view yours.

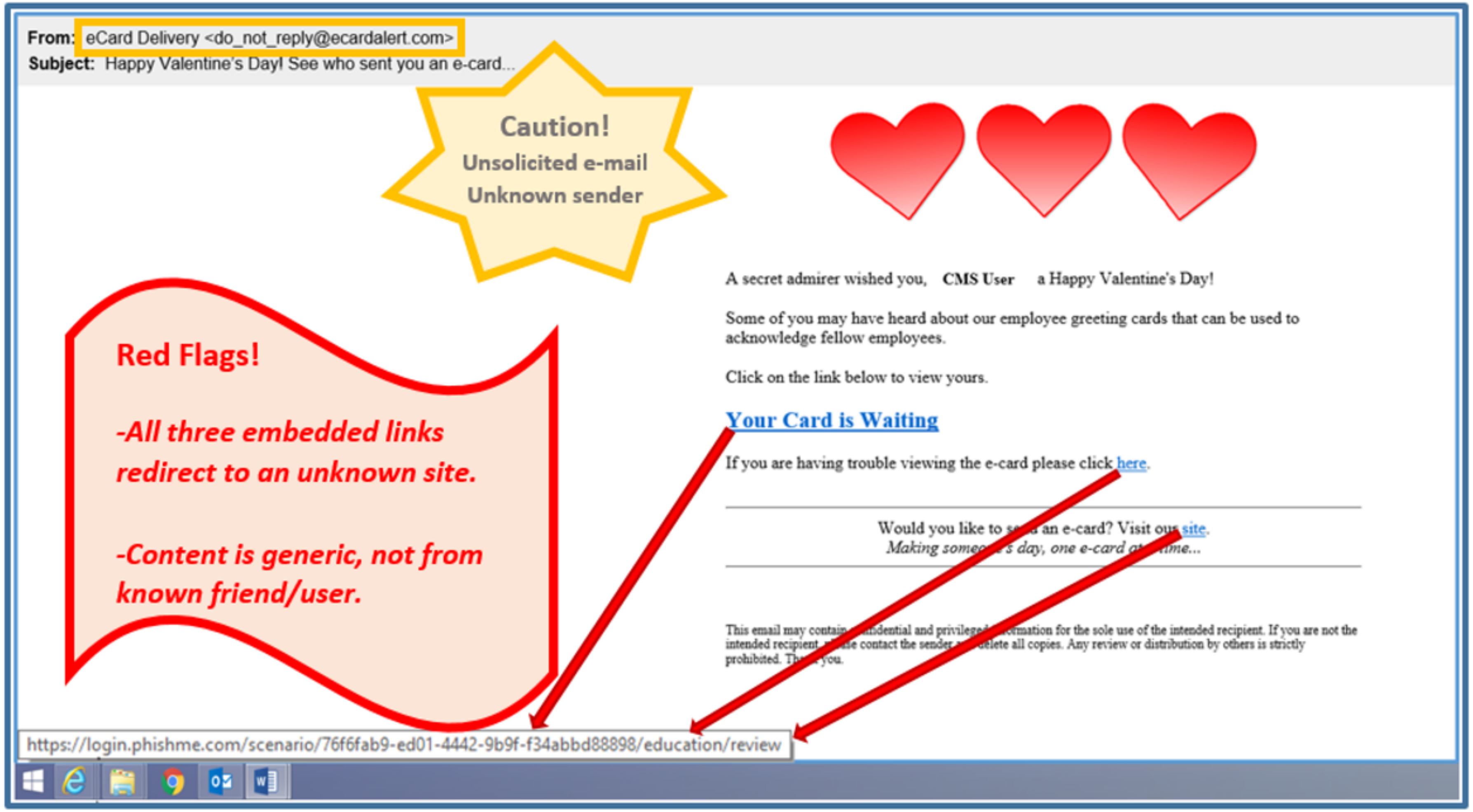
Your Card is Waiting

If you are having trouble viewing the e-card please click here.

Would you like to send an e-card? Visit our site.
Making someone's day, one e-card at a time...

This email may contain confidential and privileged information for the sole use of the intended recipient. If you are not the intended recipient, please contact the sender and delete all copies. Any review or distribution by others is strictly prohibited. Thank you.

Provide a Phishing Exercise with Follow-on Training



From: eCard Delivery <do_not_reply@ecardalert.com>

Subject: Happy Valentine's Day! See who sent you an e-card...

Caution!

Unsolicited e-mail

Unknown sender

A secret admirer wished you, **CMS User** a Happy Valentine's Day!

Some of you may have heard about our employee greeting cards that can be used to acknowledge fellow employees.

Click on the link below to view yours.

Your Card is Waiting

If you are having trouble viewing the e-card please click here.

Would you like to send an e-card? Visit our site.
Making someone's day, one e-card at a time...

This email may contain confidential and privileged information for the sole use of the intended recipient. If you are not the intended recipient, please contact the sender and delete all copies. Any review or distribution by others is strictly prohibited. Thank you.

Red Flags!

-All three embedded links redirect to an unknown site.

-Content is generic, not from known friend/user.

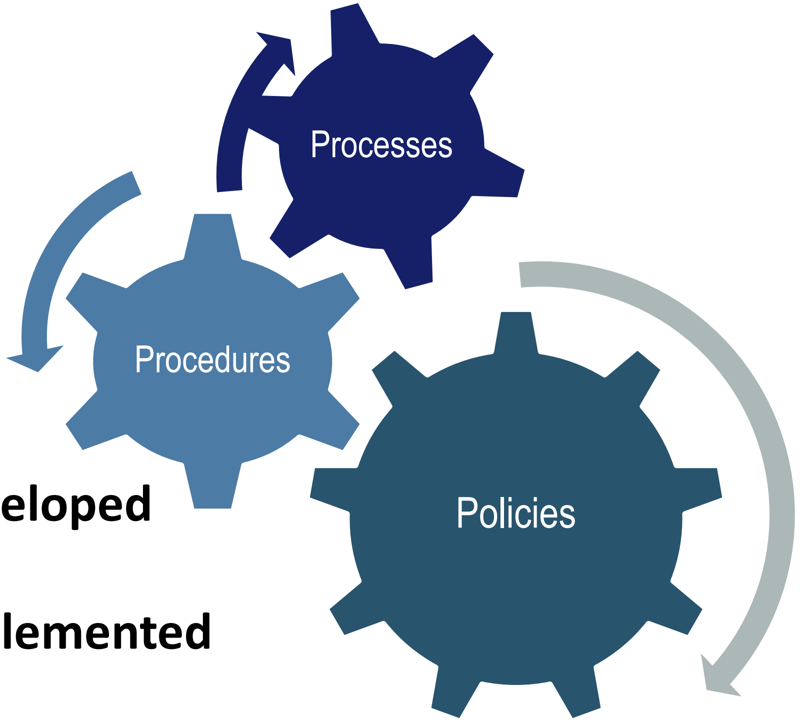
https://login.phishme.com/scenario/76f6fab9-ed01-4442-9b9f-f34abbd88898/education/review

Mitigation

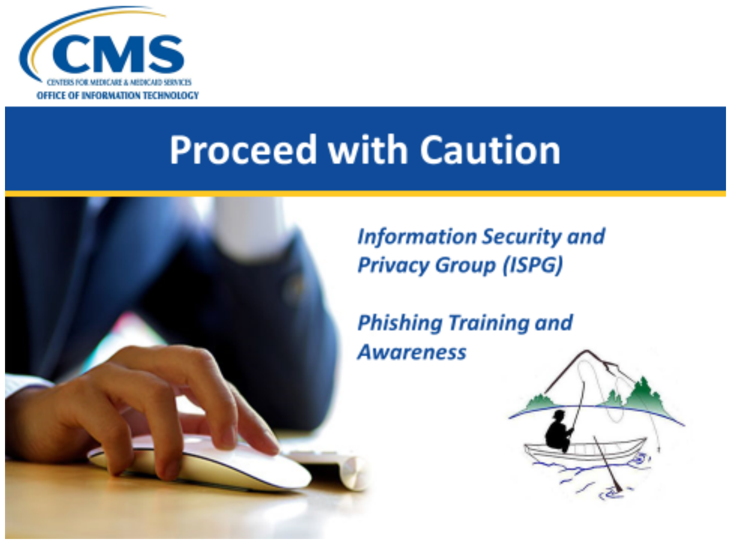
“SPAM Button” – to make it easy to report & act upon

Forward the email to HHS Spam (spam@hhs.gov) mailbox.

Acquired & Implemented Toolset



Developed and Implemented



CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION TECHNOLOGY

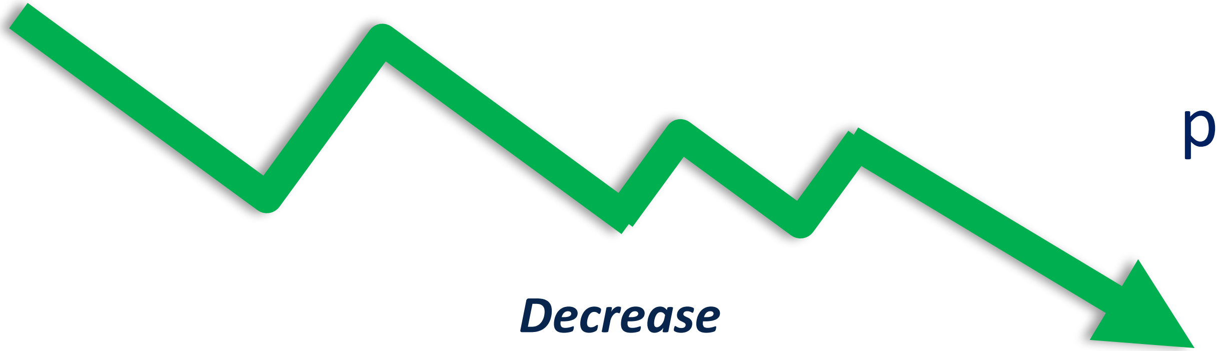
Proceed with Caution

Information Security and Privacy Group (ISPG)

Phishing Training and Awareness

Specialized training for repeat clickers

Phishing Exercises Program Outcomes



Decrease
in number of individuals that clicked
on phishing emails

41

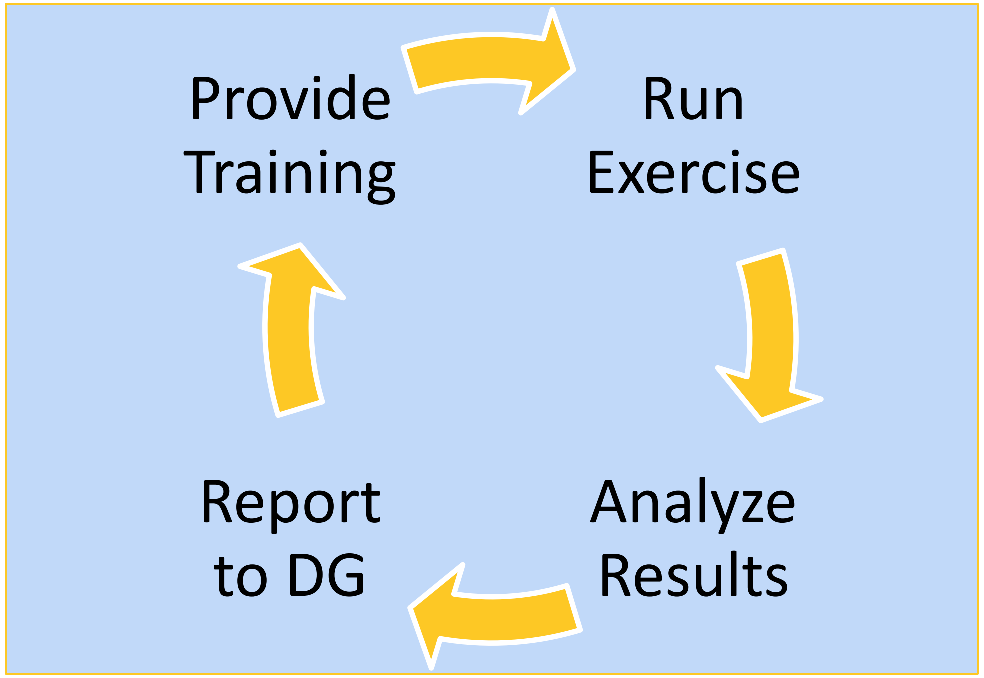
phishing exercises to date

Results:

- Improved ability by staff to identify a phishing scam
- Improved response by Security Operations Team
- Ability to focus mitigation and training

Lessons Learned

- Create a “true” baseline
- Focus on problems
  - Identification - ‘phishing clues’
  - Reporting
- Variety keeps the attention
- Communicate results of the exercises
- Follow every campaign with training


Provide Training

Run Exercise

Analyze Results

Report to DG

Incident Response Preparedness

Conduct Tabletop Exercises to:

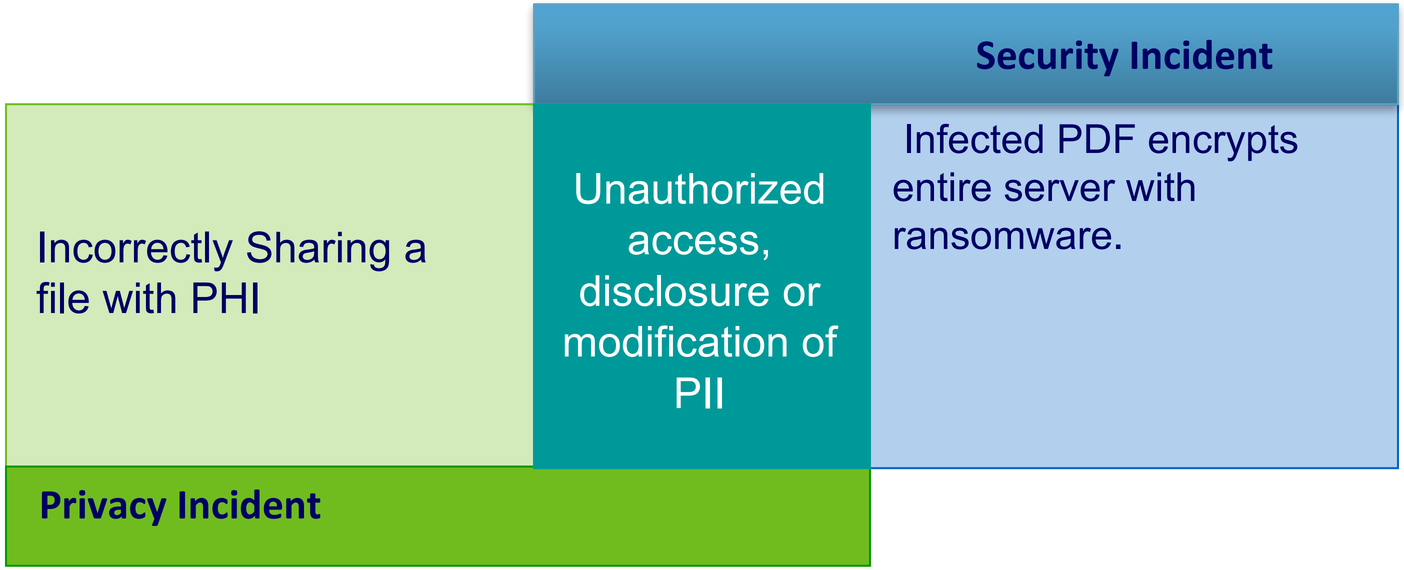
Downloaded from: http://www.eci.com

- Identify & Practice procedures
- Give input to enhance privacy/security incident response capabilities
- Identify preventative corrective actions that could be implemented

New OMB guidance recently issued emphasizes Incident Response

Develop Scenarios that
Ensure Coverage of all Types of Incidents

Not all *security incidents* are *privacy incidents*, and conversely, not all *privacy incidents* are *security incident.*



Security Incident

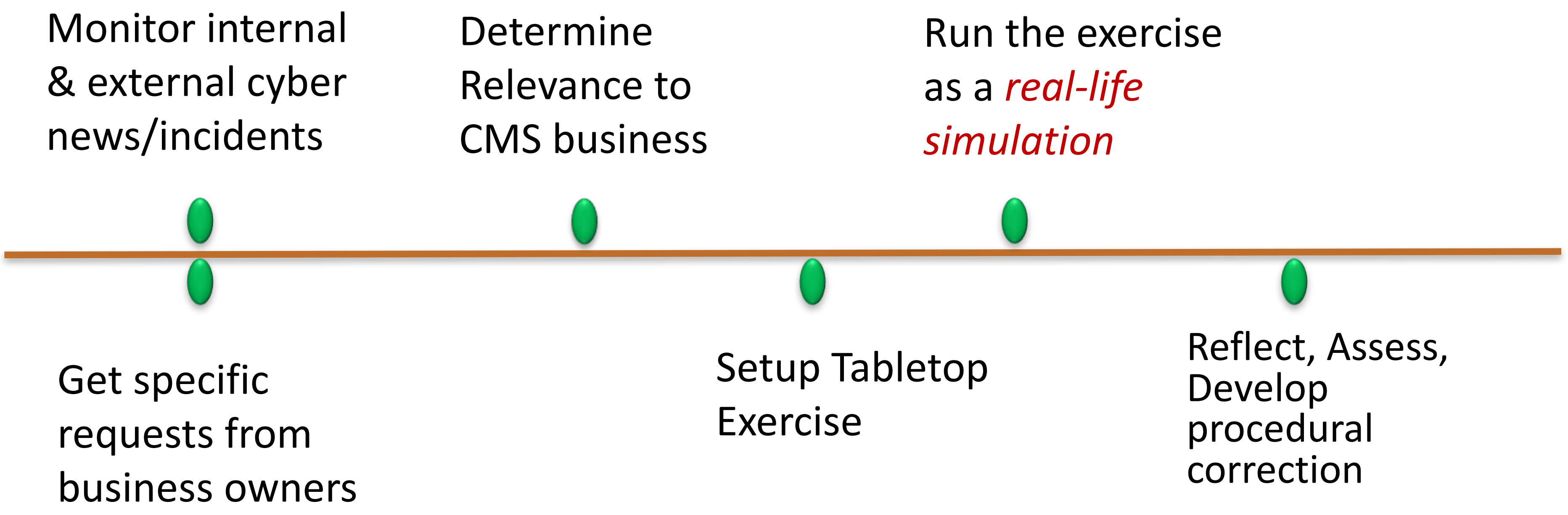
Incorrectly Sharing a file with PHI

Unauthorized access, disclosure or modification of PII

Infected PDF encrypts entire server with ransomware.

Privacy Incident

Process



Monitor internal & external cyber news/incidents

Get specific requests from business owners

Determine Relevance to CMS business

Setup Tabletop Exercise

Run the exercise as a *real-life simulation*

Reflect, Assess, Develop procedural correction

Tabletop Exercises Lessons Learned

FOCUS ON THE POSITIVE

- Solicit participant feedback on how the tabletop exercise was crafted and run – it provides valuable insight
- The results of the exercise should be analyzed on a team-by-team basis; this provides information on where gaps exist
- Use positivity and focus on insight gathered
- Build relationships and teamwork mindset

Data Guardian Program Summary

- Needs to be Business Driven focused
  - Leadership
- Data Guardian Program for communication and coordination of technology, compliance & business
- Phishing Program to anticipate threats
- Tabletop Exercises to minimize harm and facilitate recovery

Questions?

CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION TECHNOLOGY