InfoSec Training and Awareness Program

NORTHROP GRUMMAN

Training & Awareness

- Employee
- Personally Identifiable Information
- System Administrator
- Executives and their administrative assistants

Employee Comms

- Protect IT! (monthly)
- Advanced Persistent Threat (monthly)
- InfoSec Weekly News

InfoSec Intranet Site

- One-stop-shop for InfoSec training and awareness resources

Yearly Security Awareness Contest

In-person Security Awareness Events

- November Security Awareness Month

Whitepapers, Brochures

InfoSec E-mailbox

- For employee questions and feedback

Spear Phishing Exercises

- Raise awareness of spear phishing e-mail and how to properly report suspicious e-mail

Northrop Grumman has a "good user security training and awareness program" – 2010 IREC survey results

Information Security Courses

NORTHROP GRUMMAN

General User

- Information Security Awareness Annual Mandatory
- Personally Identifiable Information Protection Awareness

Role Based

- System Administrator
  - Base Course
  - Refresher Course Annual Mandatory
- Executives
  - Security Awareness Video Modules
- IT Governance, Risk & Compliance
  - Introduction to the ITGRC Required for ITGRC Users

Employee Communications

- "Protect IT!" branded monthly communication
  - Single topic; emphasis on protecting the company network and data
- Advanced Persistent Threat monthly communication
  - Single topic; emphasis on external threats to the company network and data
- InfoSec Weekly News
  - Summaries and links to external and internal news articles related to information security
- Partnerships with other internal organizations
  - Provide content for articles and presentations

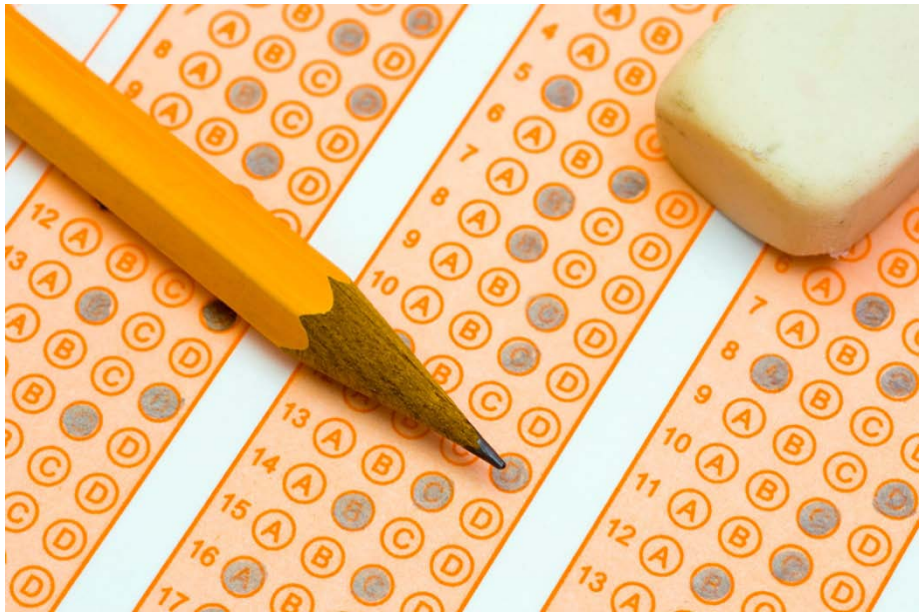
About Advanced Persistent Threat:
It's not hacking.
It's not spam.
It's espionage.

Intranet Website Includes Links to:

- Training and awareness materials
  - Internal and external articles
  - Security awareness courses
  - Videos and multimedia
  - Pages on key awareness topics
- Information on major initiatives
- Policies, procedures, and work instructions
- Organizational and contact information

Yearly Security Awareness Contest

- Ten Question Quiz
  - Questions created from information in the monthly communications
    - Links to communications provided as clues
  - Prizes awarded from imprinted giveaway inventory
  - Very popular - average 1,500 entries



In-Person Security Awareness Events

- Partnership with sector Industrial Security departments
- Company-sponsored “Security Awareness Month” every November
- In-person communication with employees
  - Answer questions
  - Provide awareness materials
  - Offer simple games in which employees can be quizzed on security awareness and win imprinted giveaways

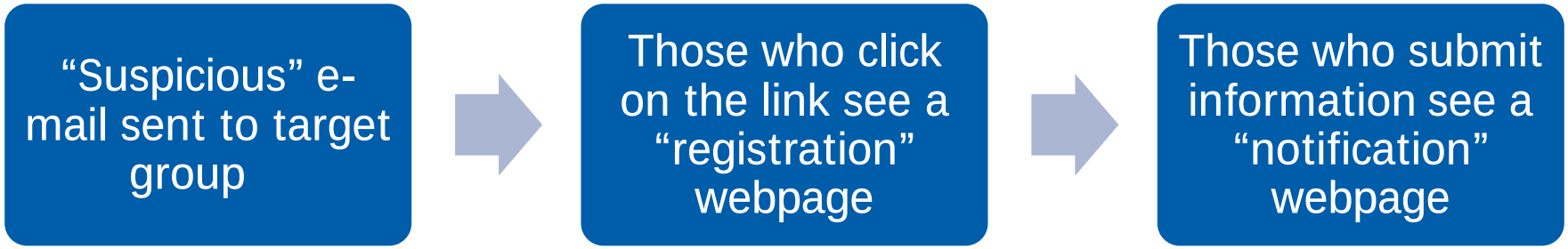
Brochures and Whitepapers

- Brochures
  - Cover key awareness topics
    - E-mail guidelines
    - Internet safety
    - Incident response for system administrators
  - Easy to hand out at in-person events

- Whitepapers
  - Cover topics more in-depth
  - Example: recommended guidelines for securing profiles on social media sites
  - Available on intranet site

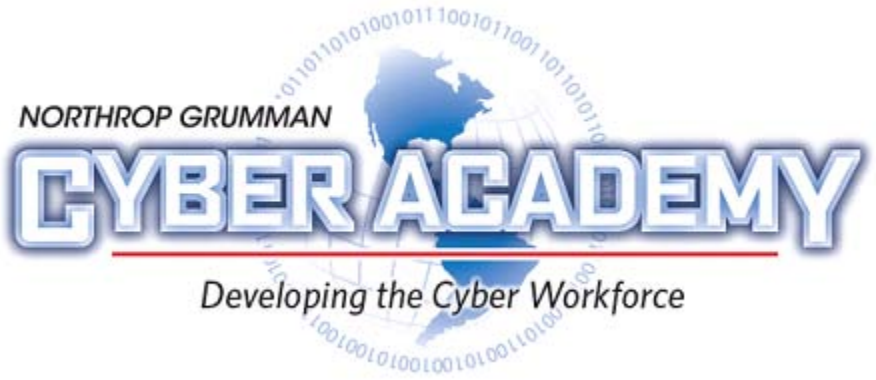
Spear Phishing Exercises

NORTHROP GRUMMAN



- The e-mail includes a link to an "unfamiliar" website
- Registration page requests personal information
- Explains the security awareness exercise

More on this later



Spear Phishing Exercises

Our Concerns

Intellectual property theft

Foreign and industrial espionage

National security

Common Spear Phishing Attacks

Username/password verification

Program information request

Industry conference information

The Problem with Spear Phishing

NORTHROP GRUMMAN

100% got through

NORTHROP GRUMMAN

Security Awareness

Spear Phishing Exercises

Objectives

Test employees' awareness of fraudulent e-mail messages

Test support groups' incident response process effectiveness

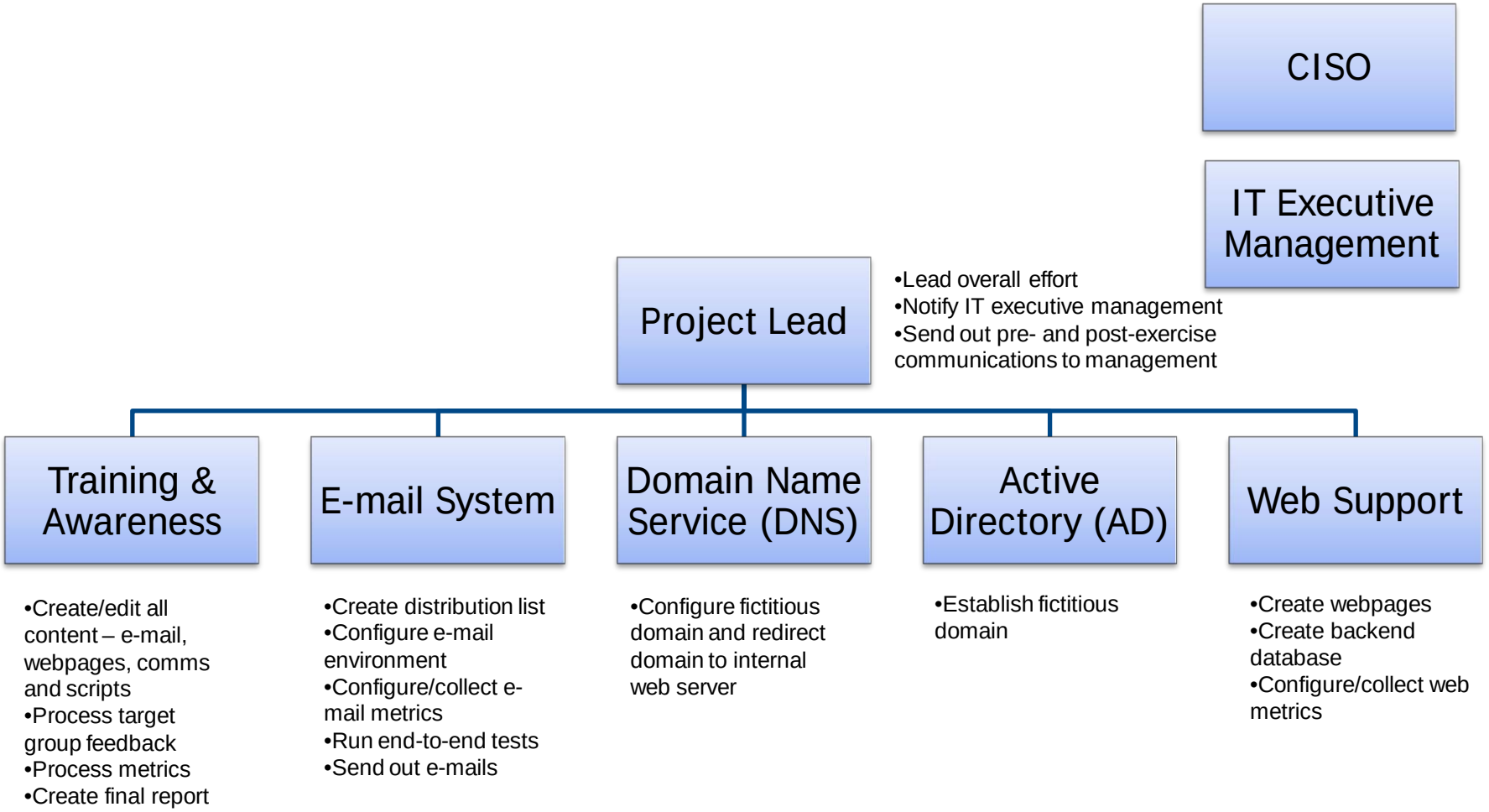
Phase 0: Initial Preparation

NORTHROP GRUMMAN

Approvals	• Who must approve a spear phishing exercise campaign?
Policies and Procedures	• Are relevant policies and procedures in place, and have they been communicated to employees?
Remedial Action Plan	• What (if any) remedial action must be taken by employees who become “victims” of spear phishing exercises?
Core Team	• Who should be included in the core implementation team?

Core Team

NORTHROP GRUMMAN



Team restricted to a minimal number to prevent information leaks

Basic Spear Phishing Exercise Model

NORTHROP GRUMMAN

E-mail

- Contains spoofed sender e-mail address
- Includes embedded URL to unfamiliar website (a fictitious domain)
- May contain other suspicious “clues”

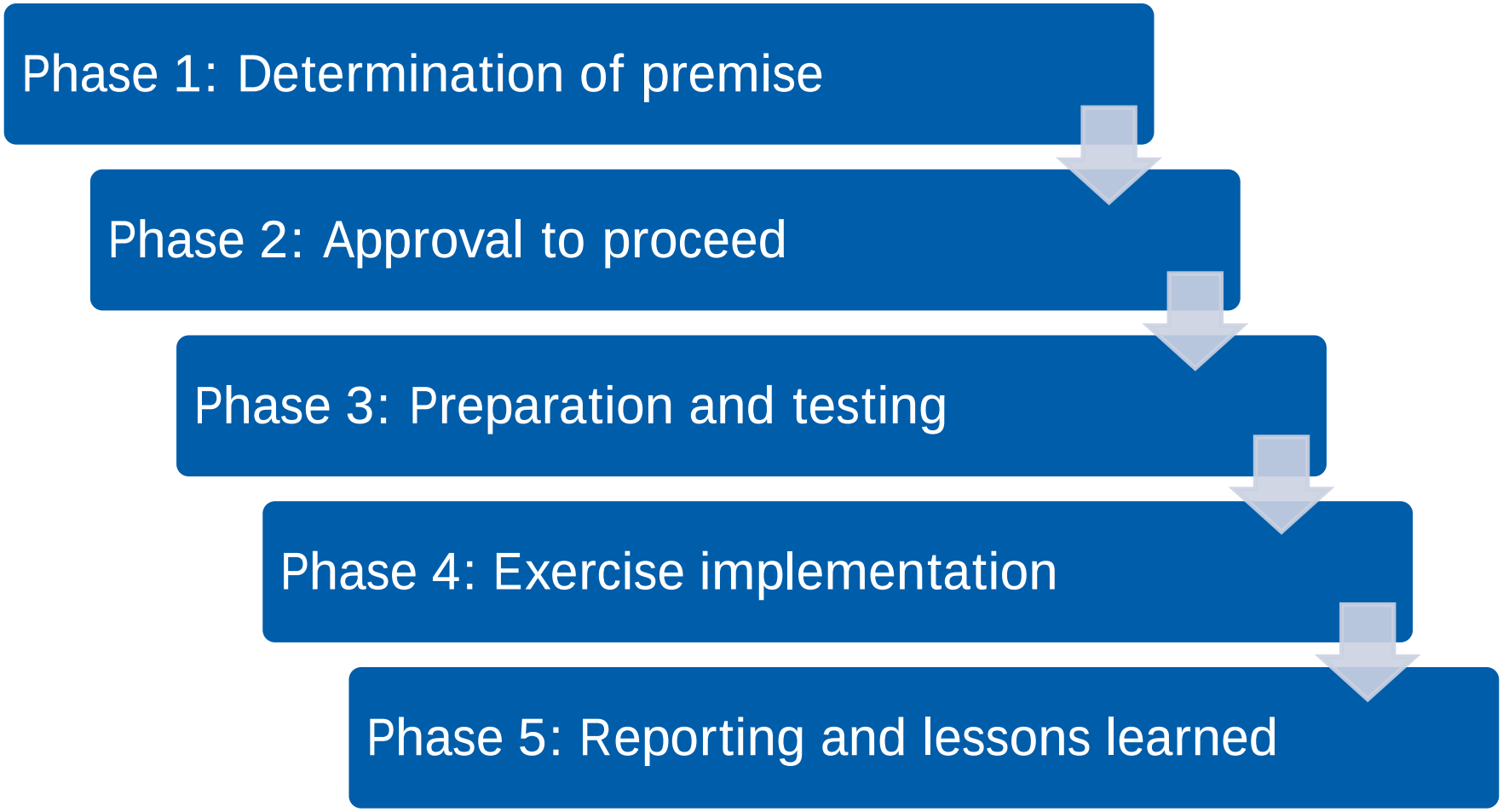
Registration Page

- Clicking to this page means the target is already “hooked”
- Requests personal information

Notification Page

- Explains the security awareness exercise
- Describes the clues
- Explains how suspicious e-mail should be reported
- Provides e-mail address for providing feedback

Exercise Phases



Phase 1: Premise

Who is the target group?

How do we “hook” them?

What clues should we include?

Premise Examples

"Verify your network account or it will be suspended"

"Last chance to receive a free encrypted flash drive"

- "Register at our site to download this whitepaper and receive a free encrypted flash drive!"

"Security Enhancement – Because of recent security threats, you must register at our site to continue to receive information from us"

"New cyber security product – register for more information"

Phase 2: Acquire Approvals as Needed

NORTHROP GRUMMAN

Target Group

Draft E-mail / Premise

Draft Webpages

Phase 3: Preparation and Testing

NORTHROP GRUMMAN

Distribution List

- Review and remove specific names if necessary

Infrastructure

- Purchase bulk mailer software
- Establish fictitious domain names
- If needed, configure perimeter e-mail environment to allow e-mails to bypass security controls
- Turn on read receipts
- Enable capture of e-mail replies and forwards

Webpage Creation

- Registration page
  - Create backend database
  - Include input validation
- On notification page, include detailed descriptions of clues and references to relevant policies and procedures

Phase 3: Preparation and Testing, cont'd

NORTHROP GRUMMAN

Communications

- Create pre- and post-exercise notifications
- Create scripts for responses from support groups
  - Ensure that users are not tipped off that a test is in progress

Metrics Collection

- Determine what metrics are needed, and make sure all metrics collection is in place
  - (More details on metrics are included on subsequent slides in this deck)

End-to-End Tests

- Verify that the entire process runs smoothly and that metrics data is captured correctly

Phase 4: Exercise Implementation

NORTHROP GRUMMAN

Send out appropriate communications after the start of the test

- Notify management that a spear phishing exercise is in progress (as needed)
- Notify support organizations after they have gone through their initial incident response process

Monitor metrics

- Have set checkpoints throughout the day to ensure that metric data is being collected properly

Determine when to shut down the exercise

- One business day is usually sufficient for metrics

Exercise may warrant sending a follow-up message to recipients for feedback

- “Why did you click or not click?”

Shut down the exercise

- Disable links to webpages
- Stop metrics collection

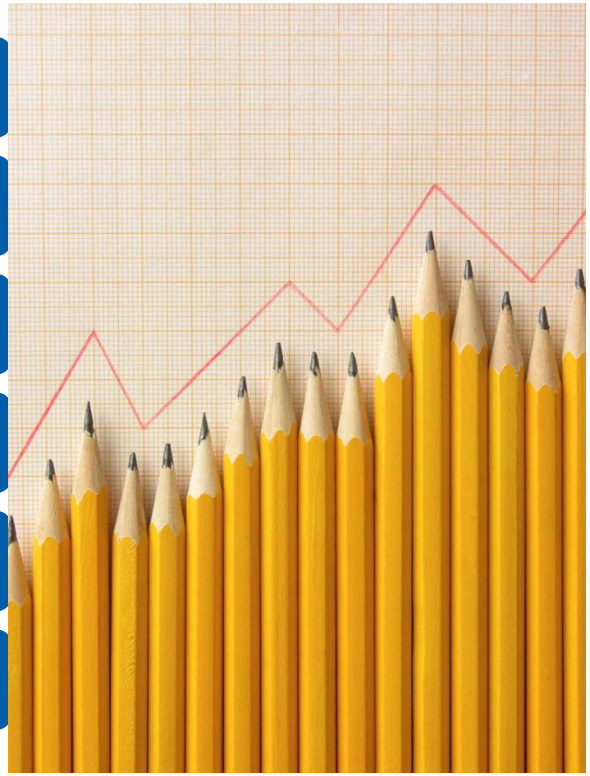
Phase 5: Reporting and Lessons Learned

- Description of test
- Presentation of metrics
- Target comments
- Lessons learned
- Recommendations
- Inclusion of screenshots of e-mail and webpages
- Summary slide of all spear phishing exercises

Example Metrics

NORTHROP GRUMMAN

- E-mails that were read
- E-mails that were deleted and not read
- Replies to e-mail
- Forward attempts
- “Victims” who clicked on the link
- “Victims” who provided personal information



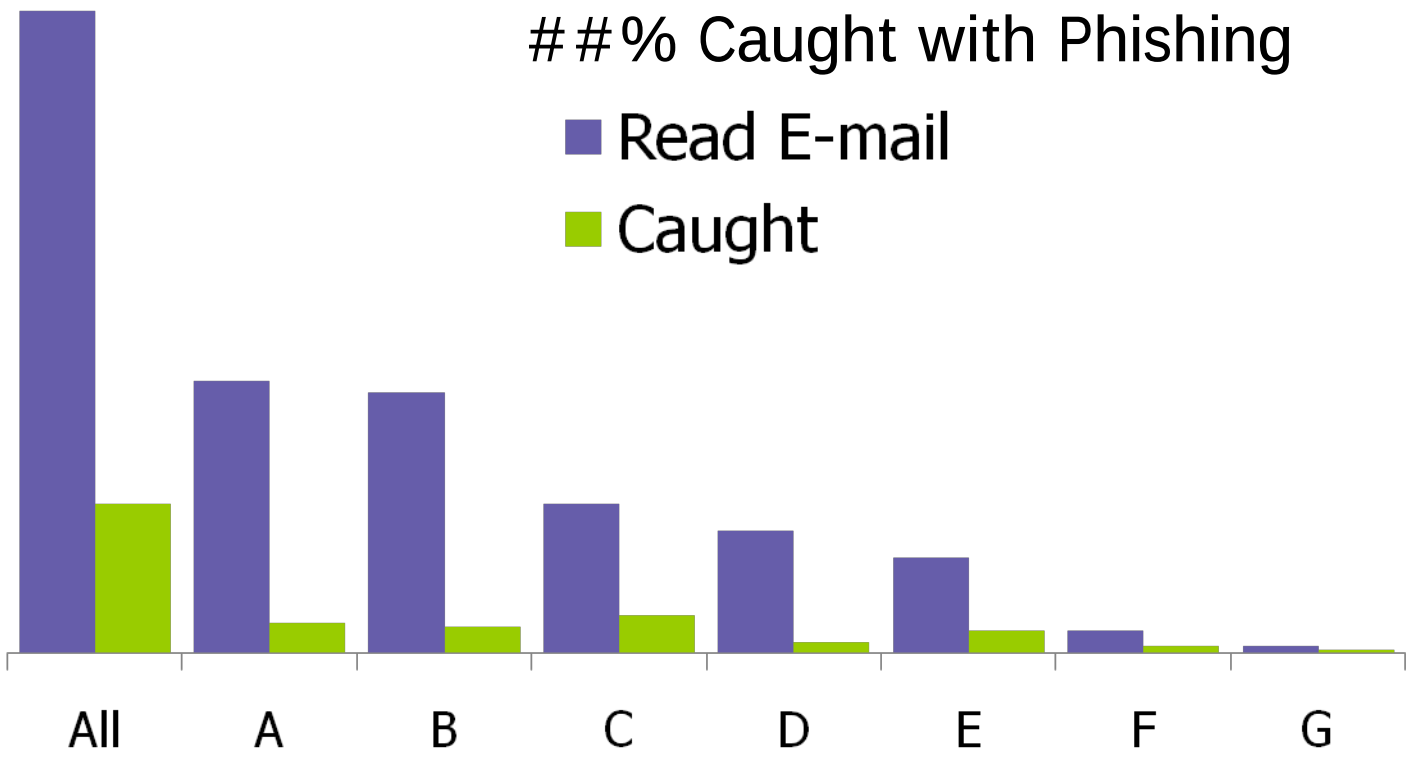
The desired metrics may dictate the parameters of the exercise

Metrics Example:
Results By Business Units “A” through “G”

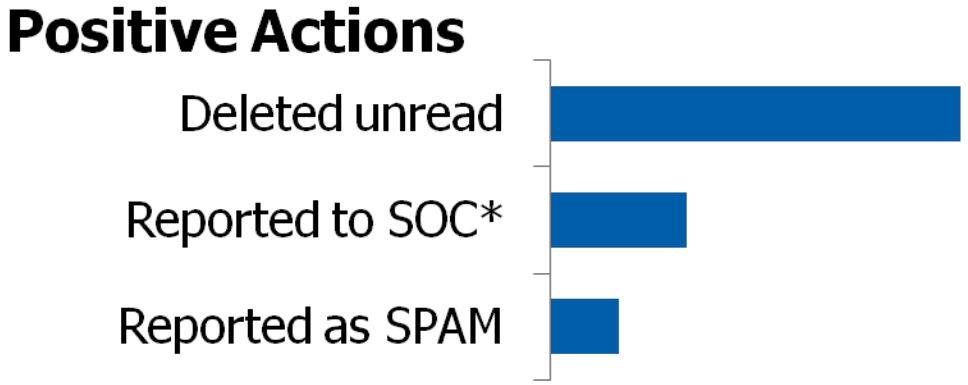
NORTHROP GRUMMAN

E-mails Sent

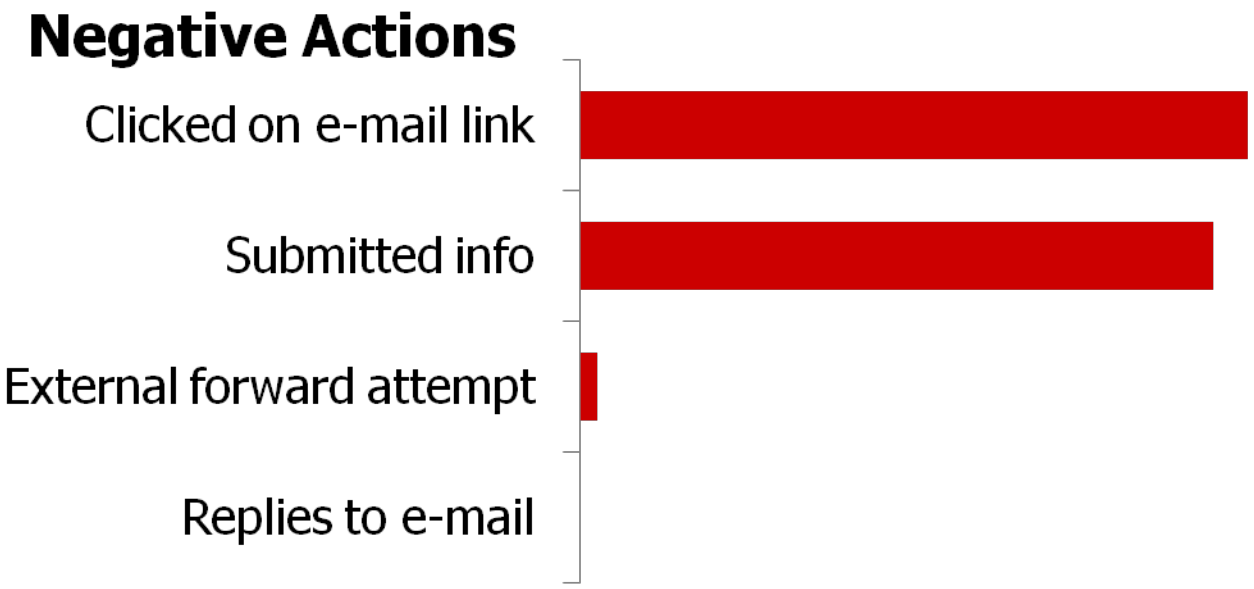
read receipts received



Metrics Example: Positive/Negative Actions



*Security Operations Center



Overall Results

NORTHROP GRUMMAN

Internal incident response teams' reaction times have improved

Feedback from "victims" has been overwhelmingly positive

Security projects have been implemented based on participants' suggestions

Lessons Learned

NORTHROP GRUMMAN

Use of registration webpage is very effective

- The victims provide more detailed personal information that can result in more granular metrics

End-to-end testing is critical

- The flow of the e-mail through the network
- The user experience of navigating the webpages
- Metrics collection

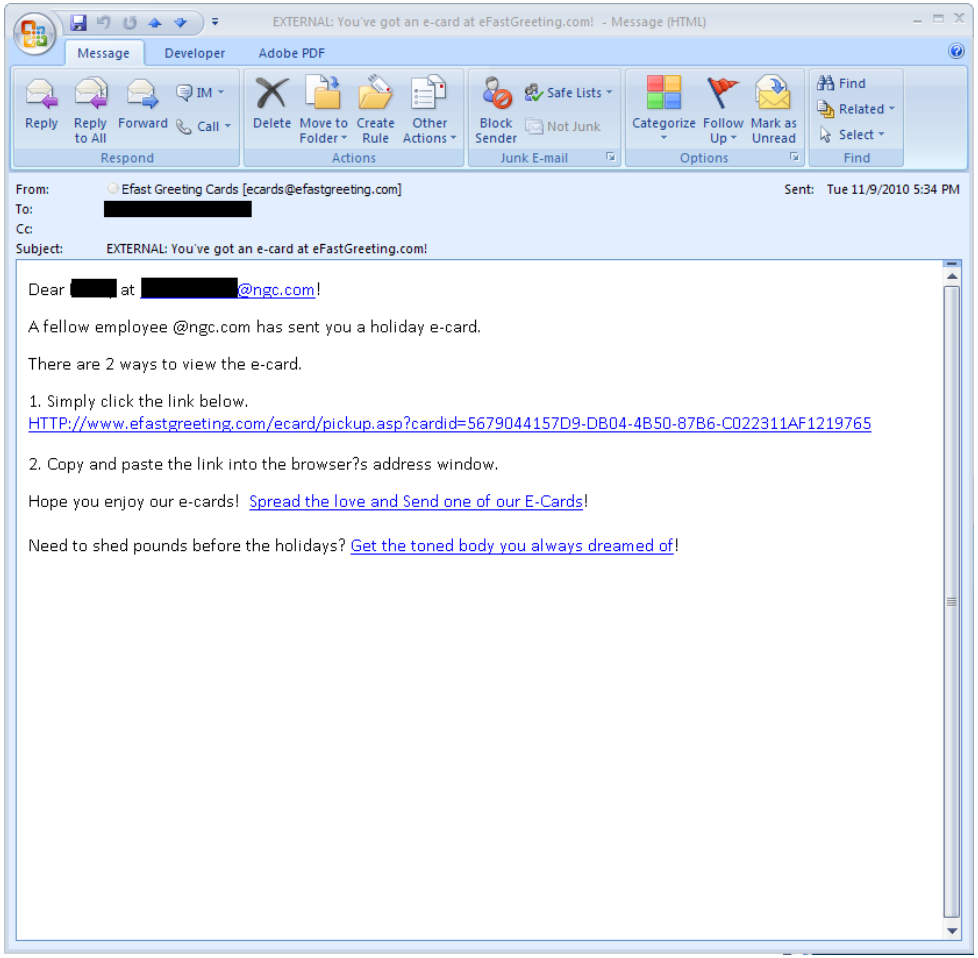
Sufficient metrics can be gathered in one day

- Eventually, victims will warn others, diluting the value of the metrics

Expect an increase in reports of suspicious e-mails

- This includes concerns that valid internal e-mails may be spear phishing attempts

Spear Phishing E-mail



Results

Conclusion

NORTHROP GRUMMAN

- Increasing security awareness does not necessarily alter users' behavior
- Implicit Cost Benefit Analysis
  - Is the cost of performing worth the return?
- How to modify inherent behavior patterns?
  - Ease of use?
  - Consequences?


NORTHROP GRUMMAN