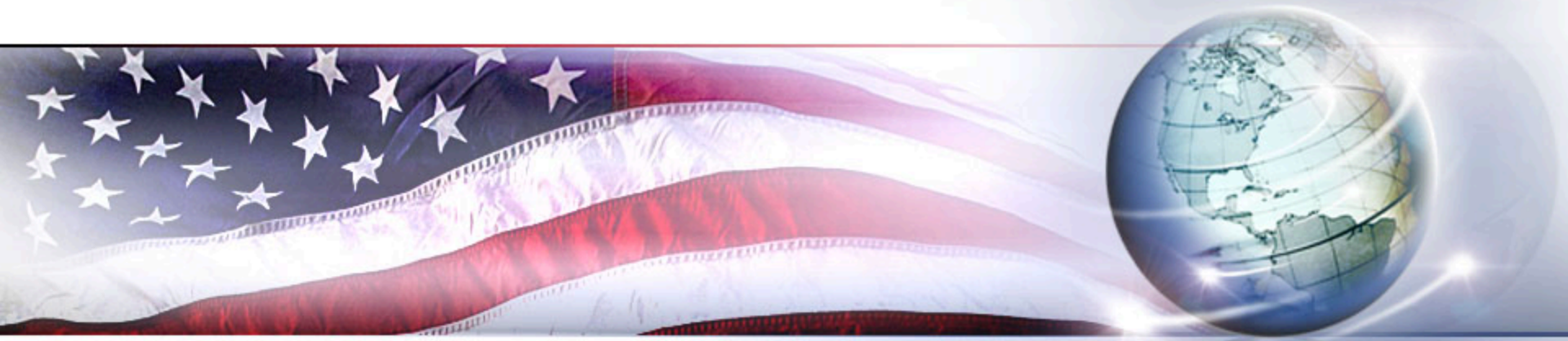
Gone Phishing, an Anti-Phishing Program Journey



Ava Logan-Woods, Information Security Specialist
Eshante Lovett, Information Security Specialist
CACI International Inc

6/19/2017

INFORMATION DEPLOYED. SOLUTIONS ADVANCED. MISSIONS ACCOMPLISHED.

CACI International Inc Overview

- Founded in 1962
- Approximately 20,000 employees worldwide with over 120 locations.
- CACI provides information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian customers.
- Member of Fortune 1000 Largest Companies, the Russell 2000 Index, and the S&P SmallCap600 Index.

CACI

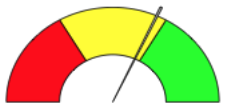
EVER VIGILANT

Overview

- Introduction
- The Journey
- Success Factors
- Setting Up the Anti-Phishing Program
- Lessons Learned
- Summary

Quick Phacts

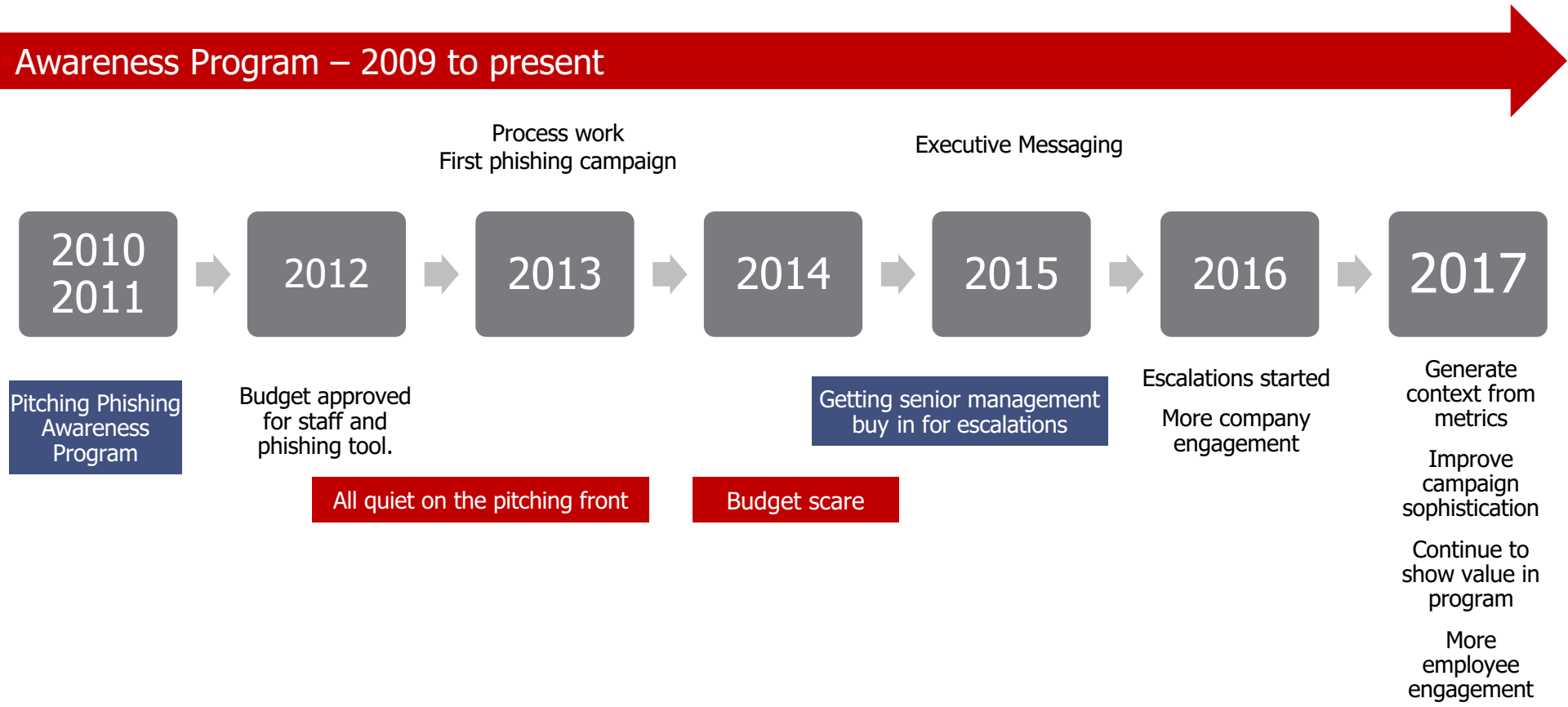
- April 2013 company baseline assessment was at a **25%** susceptibility rate.
- CACI employees have been receiving phishing awareness training for about 4 years.
- January's susceptibility rate was **2.8%**



- February's susceptibility rate was **26%**

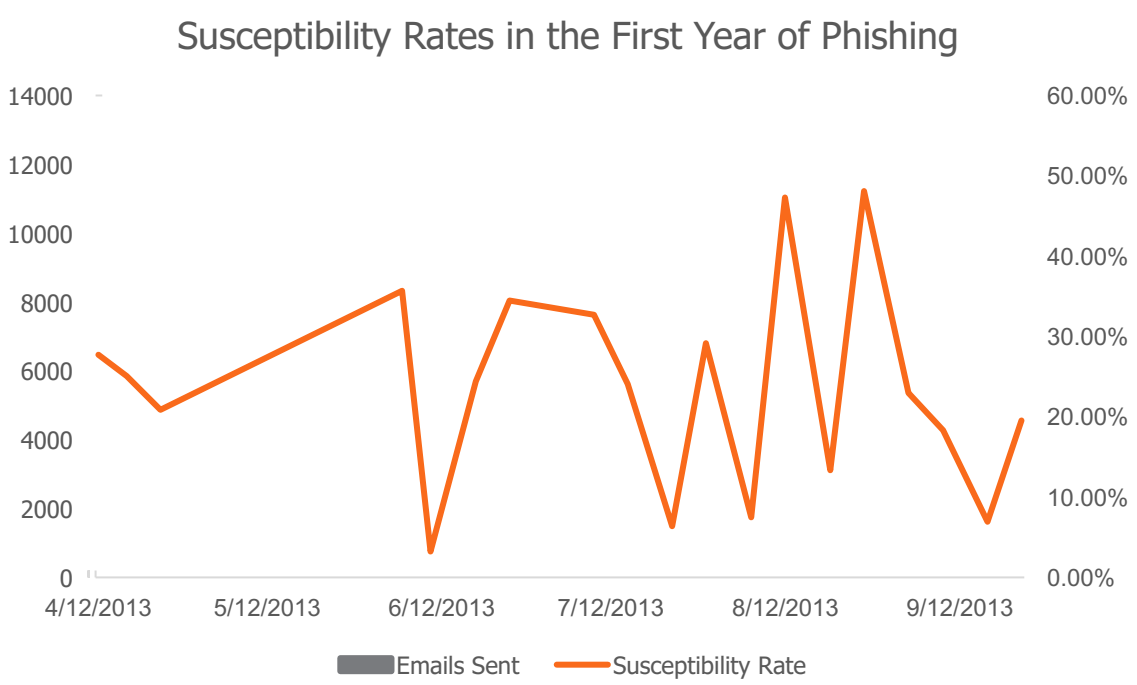
From: HR <mdexecutive@sendsecure.eu>
Subject: Attn!! W-2 Amended

CACI's Phishing Journey



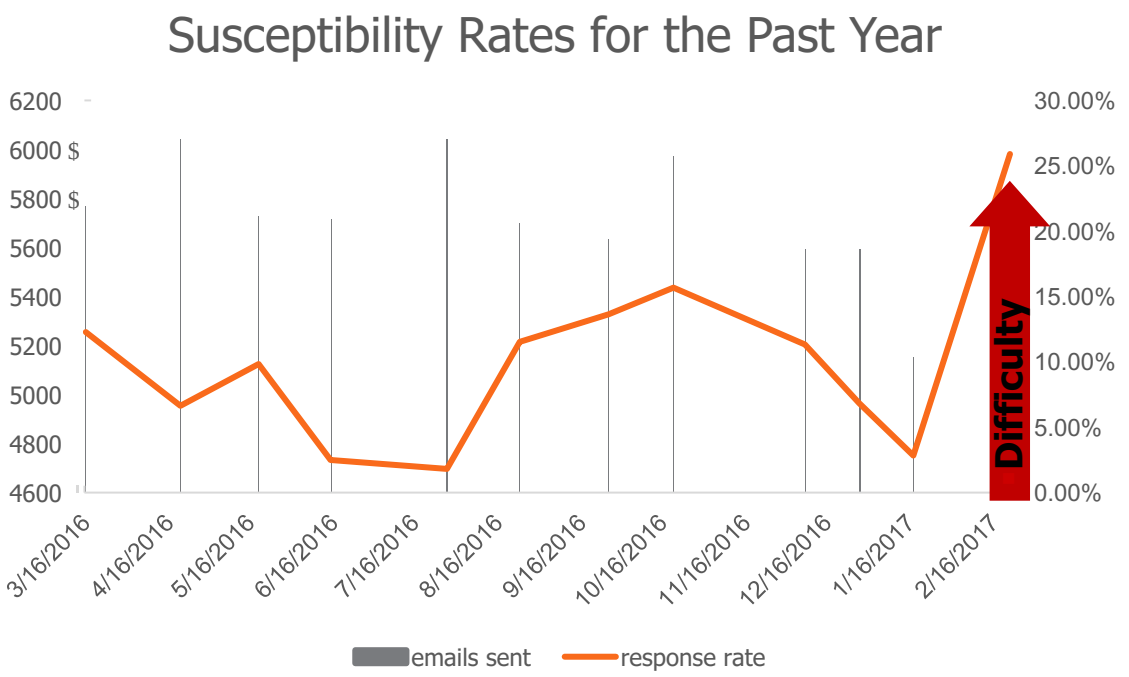
The First Phishes – Ad hoc

- **Campaigns:**
  - Varying number of emails sent over the months
  - Varying groups sent emails over different months
  - Missing months
- **Metrics Reporting**:
  - First few campaigns weren't reported up to management
  - Ad hoc, thereafter



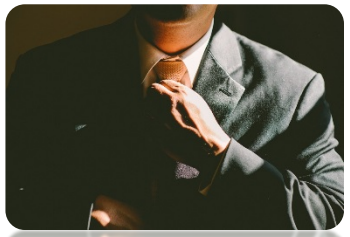
Current Phishing – Quarterly Testing

- **Campaigns**
  - Every month, 1/3 of the company is tested
  - Clickers are automatically enrolled in the next campaign (started late 2014)
  - Using real-world examples to be more relevant
- **Metrics Reporting**
  - Reporting monthly to Information Security management
  - Reporting quarterly and annually to senior management and the board of directors.



Moving the Phishing Program Forward

- **Campaigns**
  - Increase the frequency
  - Include enrolled interactive training as part of the escalation process.
  - Make reporting phishing emails easier by implementing a “reporter” button.
  - Target more susceptible populations and higher value targets
- **Metrics Reporting**
  - Providing better/more intelligence
  - Report on different susceptible populations



Success Factors

Get the Right…

People

- Executive support
- Dedicated resources on the Information Security team
- Cross-departmental resources (HR, Corporate Communications, IT, Training)

Processes & Policies

- Report a Phish process
- Escalation process
- Campaign process
- AUA and Awareness Program policy

Technology

- Leveraged mail analysis tool for program justification
- Building campaigns
- Training & Communication
- Data compilation and analysis

Setting Up CACI's Anti-Phishing Program

1. **Recognize the risk**
2. **Lay the foundation – getting others to recognize the risk**
3. **Lobby for resources**
4. **Scan the market, in-house or vendor provided tool, understand requirements, what would it look like?**
5. **Flesh out the implementation plan**
   - How will you integrate this program?
   - Consider staffing – there is work before, during, and after the campaign
   - First processes planned; experience changes things
6. **Phish & Report - this will evolve over time.**
7. **Continuous Improvement**

Lessons Learned

- The first test set the tone for what needed to be done. Each time we phished, we learned more.
- Never underestimate collaboration with the IT department .
- Some groups needed to be excluded.
- Consequences of reporting training results - these are humans.
- Sophistication levels need to be fleshed out and change over time.
- The anti-phishing program is a living, changing thing.
- Success isn't solely based on low click rates.
- Escalation is controversial.
- Tracking the data is crucial.
- Keep up the hype.

The technology doesn't make the change, it's the vehicle to touch the users directly

How to Spot Success

- **Getting Buy-in**
  - Blog
  - Community of Practice
- **Money for swag**
- **Corporate messaging is getting more attention**
- **More engagement with employees**
  - People reporting – “I Clicked!”
  - “I got this email that’s a bit suspicious…..”
- **Fewer angry emails; More pleasant emails**

"KEEP SENDING CRAP ON MY $
GOVERNMENT COMPUTER AND I WILL $
KEEP OPENING IT UNTIL THE $
GOVERNMENT CONTACTS YOU" $

"Thank you very much for the notice. I was on vacation last week when I rec'd this message and I clicked on it from my phone and knew it was a mistake immediately. I intended to send a message to <incident response email> to let you know of my error but am still digging out from work emails. I have read info below and completely understand the importance of this topic and will exercise extra diligence going fwd (even on vacation)." $

Summary

- The beginning of our program was all about learning and we continue to do so.
- You're in it for the long haul … the program doesn't change things overnight.
- Promoting the program is critical to its success – share wins
- The Anti-Phishing Program has helped promote the Information Security team, influence policy, increase interest in the Awareness Program, and improve relationships.
- The Information Security team is seen as more accessible now.

REVIEW AND DELETE THIS NOTE - Use this slide for presentations with multiple sections

Main Title Placeholder

Section Title Placeholder

Text area options include adding:

- Photo caption
- Subtitle
- Website reference
- Quote
- Section number
- Other

Photo area options:

- Use this standard flag as a default image and delete this note
- Replace this image with another relevant content image and delete this note

Presenter Name
Presenter Title
Date