YEAH, I HAVE A POWERPOINT...

DEVELOPING AN INFORMATION SECURITY AWARENESS PROGRAM

By: Marcia Mangold

DESIRED LEARNING OUTCOMES

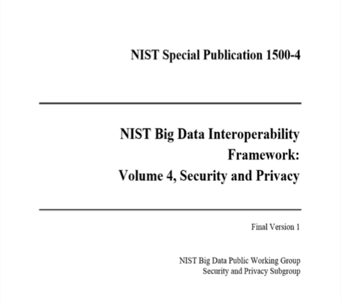
❑ Understand the difference between “Compliance” and “Security” for information awareness training

❑ Understand the lifecycle of an Information Security Awareness Training program

❑ Examples of low-cost ideas for awareness training communications, events and activities

Marcia Mangold

BCBSM & BCN INFORMATION SECURITY



NIST Special Publication 1500-4

NIST Big Data Interoperability Framework:
Volume 4, Security and Privacy

Final Version 1

NIST Big Data Public Working Group
Security and Privacy Subgroup

HENRY FORD COL
FUTURE

WALSH® COLLEGE

UNIVERSITY OF DETROIT MERCY
1877 1941

CISSP®

TOASTMASTERS INTERNATIONAL

IBM

GE

Blue Cross Blue Shield of Michigan

HENRY FORD COMMUNITY COLLEGE
1938

GM

ciena

SECUREWORLD DETROIT

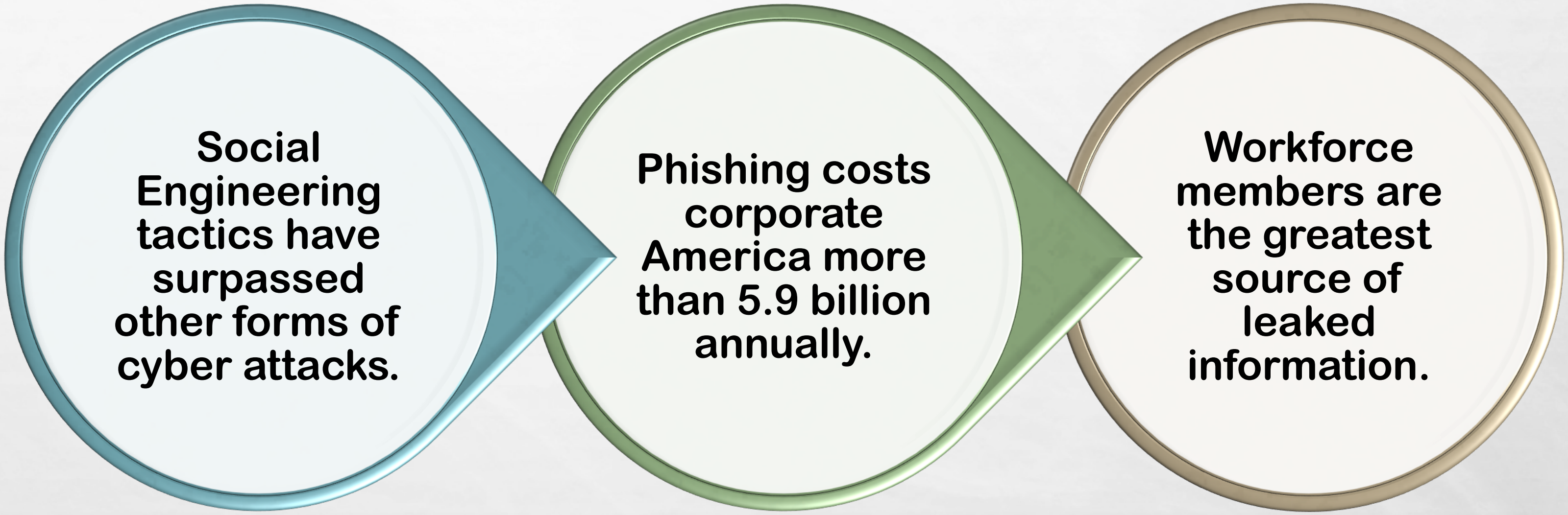
WXW
Women's Exchange of Washtenaw

fissea

ISSA
Information Systems Security Association International
www.issa.org

(ISC)²
CHAPTER
GREATER DETROIT

WHAT WE ARE FACING…



Social Engineering tactics have surpassed other forms of cyber attacks.

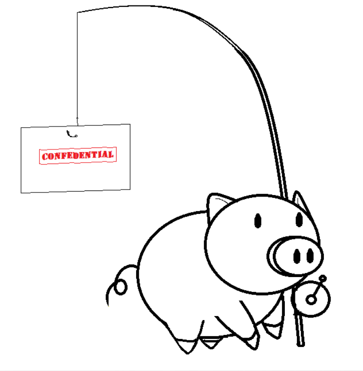
Phishing costs corporate America more than 5.9 billion annually.

Workforce members are the greatest source of leaked information.

Phishing and social engineering threats are no longer limited to e-mail and include methods such as: Person to Person, SMS messaging (smishing) , voice phishing (vishing), and portable media.

More mandates and frameworks require IS Awareness Training…

WHAT IS AT STAKE…



Impact of an attack

- Reputational damage
- Time ($$$) lost due to service disruption and remediation
- Loss of intellectual property and sensitive business information
- Potential financial loss
- Affect on National Security

- **On average, 30% of phishing emails are opened.**
- **The #1 delivery vehicle for malware is phishing messages.**
- **89% of breaches had a financial or espionage motive.**

– Verizon Data Breach Investigations Report 2016

COMPLIANCE VS SECURITY

Compliance	Information Security
A state of being in accordance with established guidelines, specifications or legislation or the process of becoming so	Measures taken to guard against espionage or sabotage, crime, attack, or loss.
Doing what is necessary to meet an audit or regulatory compliance.	Doing what is necessary, to reduce risk to an acceptable level.

"being compliant" does NOT guarantee that "something is secure"

WHY AWARENESS TRAINING WORKS

An Information Security training program:

- Addresses your company’s interpretation of applicable security policies, guidelines and regulations
- Supports the business’s activities that mitigate risk
- Measures security based upon the results of baseline assessments, and support IS policies

With Continuous and Varied Security Awareness training, Employees:

- Learn to recognize malicious exploits and how to counteract them
- Are reminded that Information Security Awareness is an every day activity, not just a “training” taken once a year
- Become “Front Line Defenders”, instead of “Hackable Humans”

“Employee training and awareness continues to be a critical – and often neglected – component of cybersecurity.” from US cybersecurity: Progress stalled Key findings from the 2015 US State of Cybercrime Survey, July 2015

POWERPOINT VS A TOOL

Traditional Awareness Training

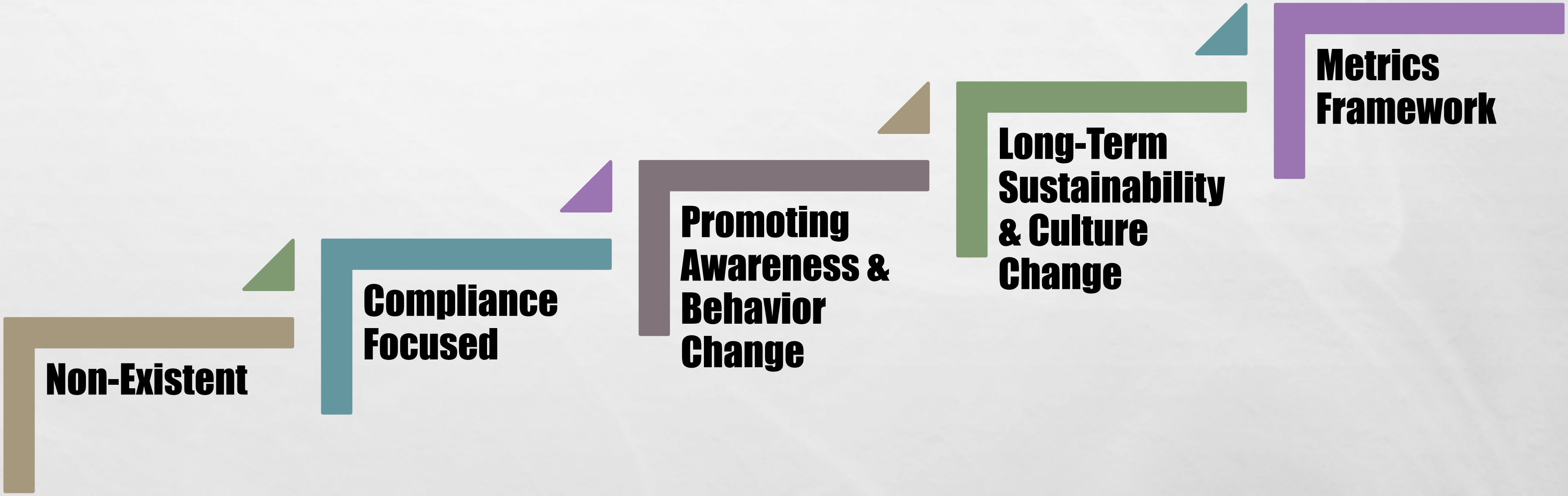
- PowerPoint presentation once a year, supplemented with posters, email alerts, and videos.
- Satisfies compliance

What the experts are saying. What the vendors are trying to sell you

- The vendors try to sell you a “tool” for your information security awareness training.
- A tool only addresses one aspect of your training needs.
- Use vendors as a partner in creating your awareness training program.

What you really need is an Awareness Training Program

INFORMATION SECURITY AWARENESS TRAINING PROGRAM ASSESSMENT

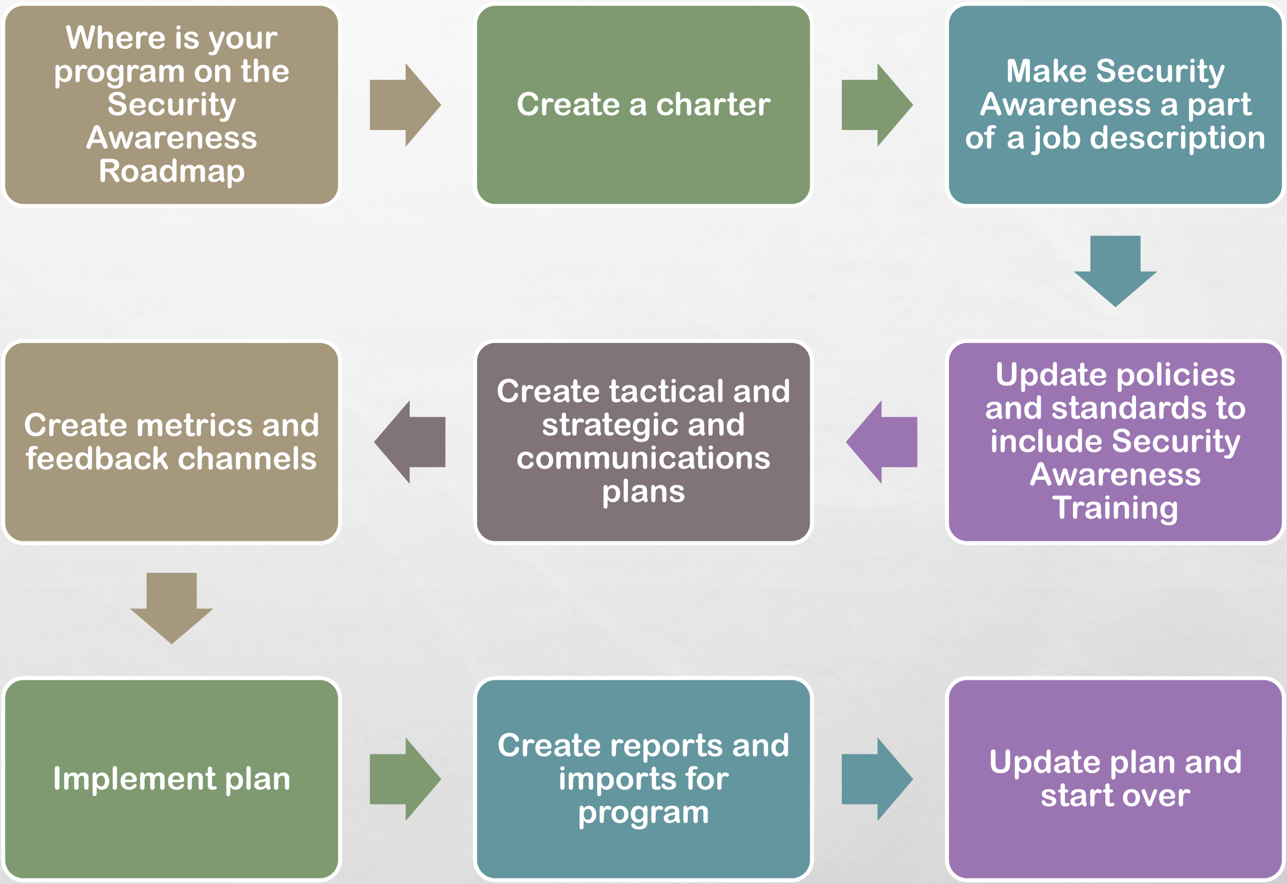


- Non-Existent
- Compliance Focused
- Promoting Awareness & Behavior Change
- Long-Term Sustainability & Culture Change
- Metrics Framework

Security Awareness Maturity Model

Where are you? And Where do you want to be?

LIFECYCLE OF AN INFORMATION SECURITY AWARENESS TRAINING PROGRAM



Where is your program on the Security Awareness Roadmap

Create a charter

Make Security Awareness a part of a job description

Update policies and standards to include Security Awareness Training

Create tactical and strategic and communications plans

Create metrics and feedback channels

Implement plan

Create reports and imports for program

Update plan and start over

How do you get there?

IN THE BEGINNING

Create a charter

- Gain buy-in and funding
- Shows that you are serious
- Base program on your internal culture, frameworks, best practices, along with compliance needs

Make Awareness Training a part of a job description

- Make it a part of your yearly goals
- Leadership sponsorship
- Training opportunities

Update policies and standards to include Security Awareness Training

- Shows everyone else that you are serious
- Lets everyone know what is expected

Create tactical and strategic, and communications plans

- Outlines your program and goals to get to the next level
- Gives you a timeline
- Use for budgeting and funding
- Determine who you can partner with inside and outside of the organization
- Determine how you will get your message out
- Determine who needs to know what and when

WHAT'S IN YOUR PROGRAM?

- Partner with other initiatives
- CyberSecurity Month

Events, contests and workshops

- Secure coding training
- Phishing Victims
- Sales & Marketing
- CSRs

Specialized training based on role, job description

- First phish spotter
- Surveys
- Contests

Rewards

- Phishing, vishing, smishing, piggybacking, scams, physical safety, etc.

Emails, articles, videos, testing

- Offer to present at team meetings
- Create Customized training

ATaaS Awareness Training as a Service

- InfraGard, ISSA, ISACA, ISC2, Secureworld

Partnering with other areas inside and outside of the organization

- CBT and Compliance Training
- Sensitive information check (clean desk)

On going Employee assessment program

Remember to "Make it PERSONAL"

IMPLEMENT REPEATABLE PROCESSES…

Rollout Step	Description
Set-up	Create environment, create roll-out schedule, develop metrics, and create use cases for pilot
Pilot	Structured testing of delivery, and actions, using security department resources
Communications	Communications plan and roll-out of initial information to department heads, helpdesk and selected IT
Phase	Perform activity
Retest	Optional activity to determine effectiveness of training.
Metrics, reporting, etc.	Review metrics and combine findings into a report that will be used for awareness training

Since you have to be compliant, start with policy and create "repeatable" processes

REPORTING RESULTS…

Create metrics and feedback channels

- What do you need to know
- What do others need to know
- Use surveys, interviews, etc.

Create reports

- Customize the reports based on the audience
- Think about what needs to be changed, improved or eliminated

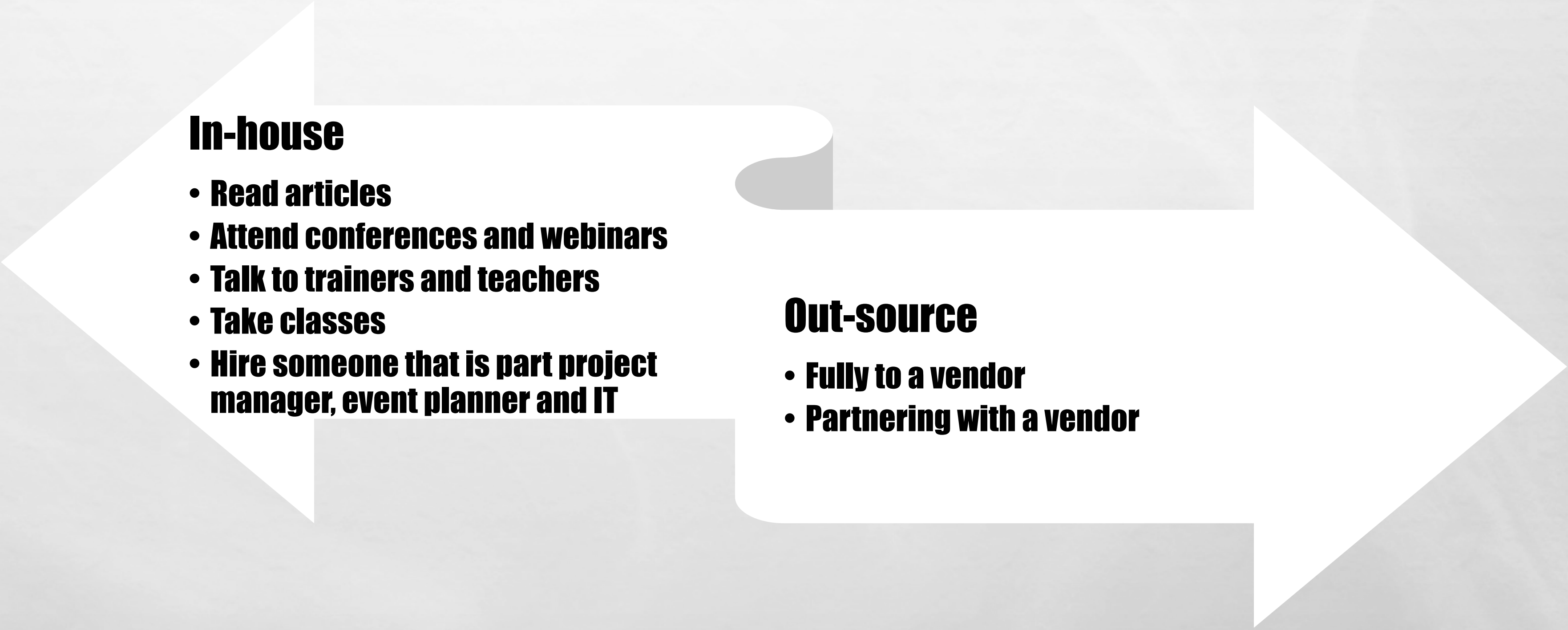
The metrics and reports should be based on your goals for the program, actual results that can be supported, and the audience

BRINGING IN THE CROWD…

- PRIZES OF UNTOLD VALUE!
- SOMETHING THEY CAN USE AT HOME
- SOMETHING THEY CAN SHARE
- SOMETHING THEY WILL REMEMBER

If Possible, make it FUN!

GETTING THE SKILL SETS THAT YOU NEED TO BE SUCCESSFULLY



In-house

- Read articles
- Attend conferences and webinars
- Talk to trainers and teachers
- Take classes
- Hire someone that is part project manager, event planner and IT

Out-source

- Fully to a vendor
- Partnering with a vendor

RESOURCES

FREE

SANS	•https://securingthehuman.sans.org/ •Posters •Strategy
KNOWBe4	•https://www.knowbe4.com/ •Scam of the week •CyberheistNews
Dark Reading	•http://www.darkreading.com/ •Webinars and News
SearchSecurity.com	•http://searchsecurity.techtarget.com/ •Webinars and News
YouTube	•http://youtube.com •Videos •Ideas

LOW COST IDEAS

□ Partnering with other areas, such as communications, physical security, compliance and even facilities

□ Ice cream socials, afternoon tea, morning coffee, salsa or chili contest

□ Unbreakable password contest

□ Caught you doing something right

PUTTING IT ALL TOGETHER

The difference between compliance and security for Information Awareness Training is that your training program should not stop at checking off the boxes

Create an Information Security Awareness Training Program with a lifecycle

Explore low-cost ideas for Awareness Training communications, events and activities

Make it personal

Remember to have FUN!

Q&A