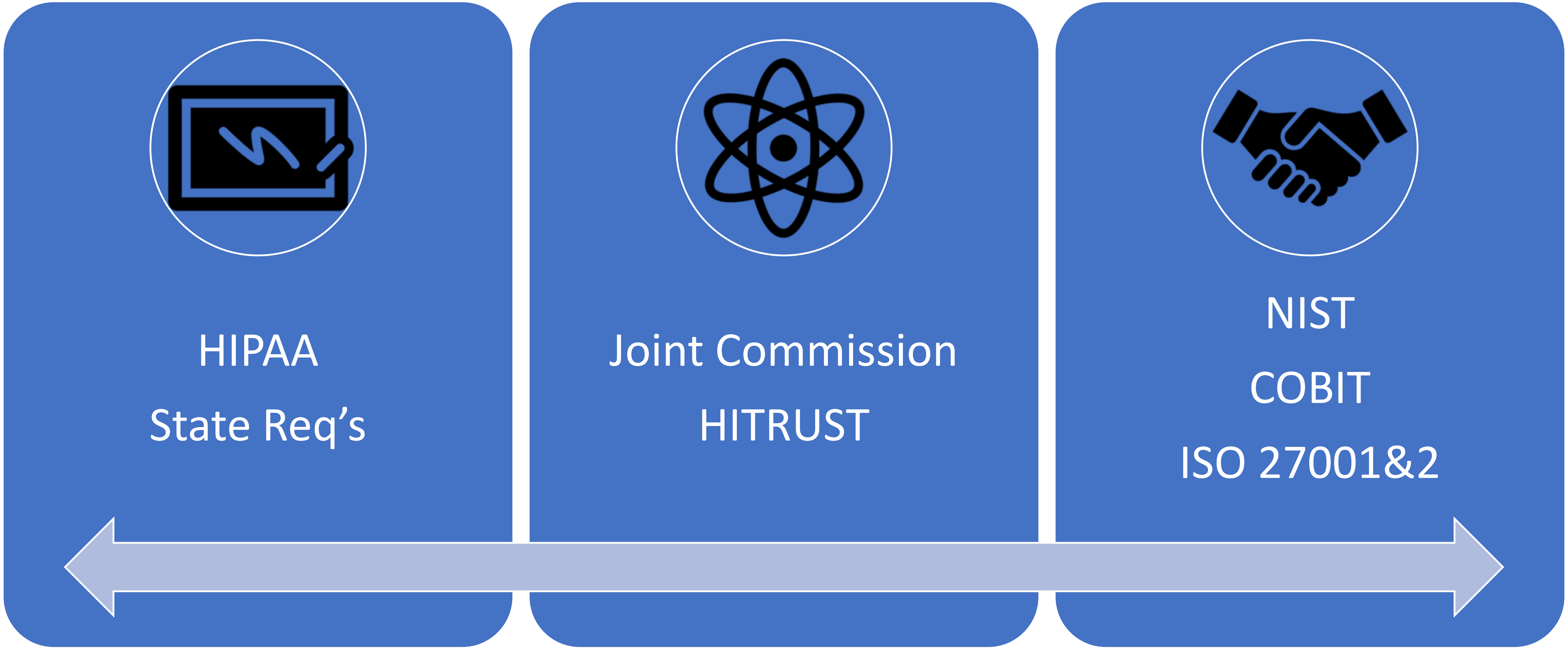
InfoSec Training & Awareness: Your First Line of Defense

By: Jason Griffin, CISM

Agenda

- Overview of compliance requirements
- Strategies for determining appropriate training approaches
- Operationalizing training strategies
- Measuring Success
- Q&A

Training….As a matter of compliance/certification/framework



HIPAA

State Req's

Joint Commission

HITRUST

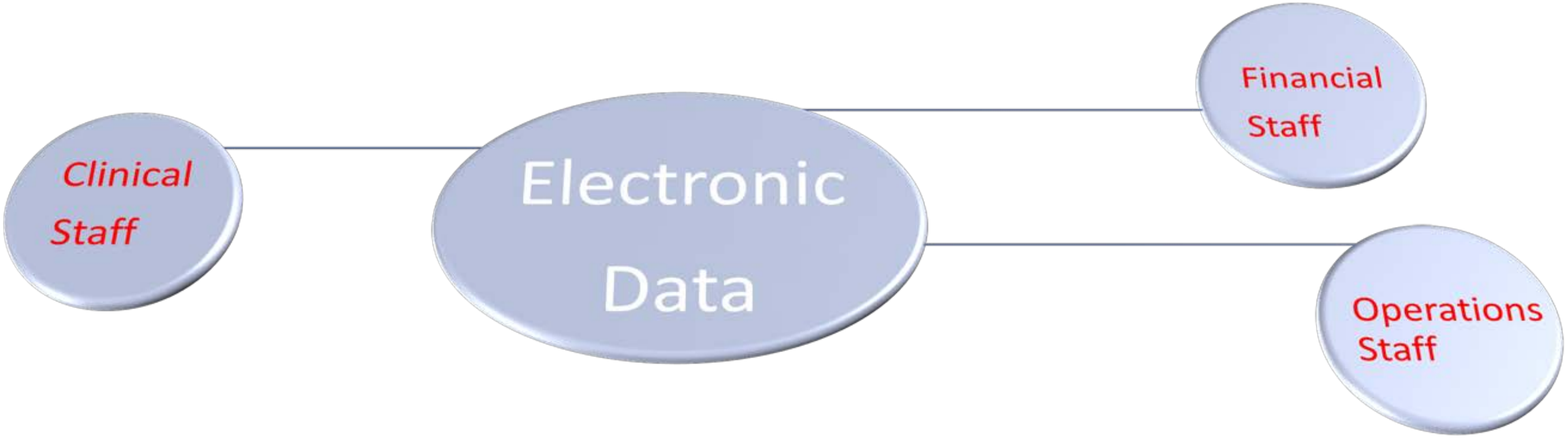
NIST

COBIT

ISO 27001&2

First Critical Control

- **Security awareness & training** is one the most critical elements to your security program because it accelerates your ability to identify threats and improves the consistency of implemented security controls.
- Every person in your organization is an intrusion detection point



Training & Awareness

The **goal of awareness is to raise the collective awareness of the importance of security and security controls.** Awareness messages should be simple, clear and easily understood by the audience.

The **goal of training is to facilitate a more in-depth level** of user understanding

- SANS Institute

Strategies and What to Avoid

Teaching an old dog, new tricks

Security is an information technology problem, not mine

Implementation of new technology

One-size-fits-all

Too much information

Lack of organization

Failure to follow-up

Getting the message where it counts

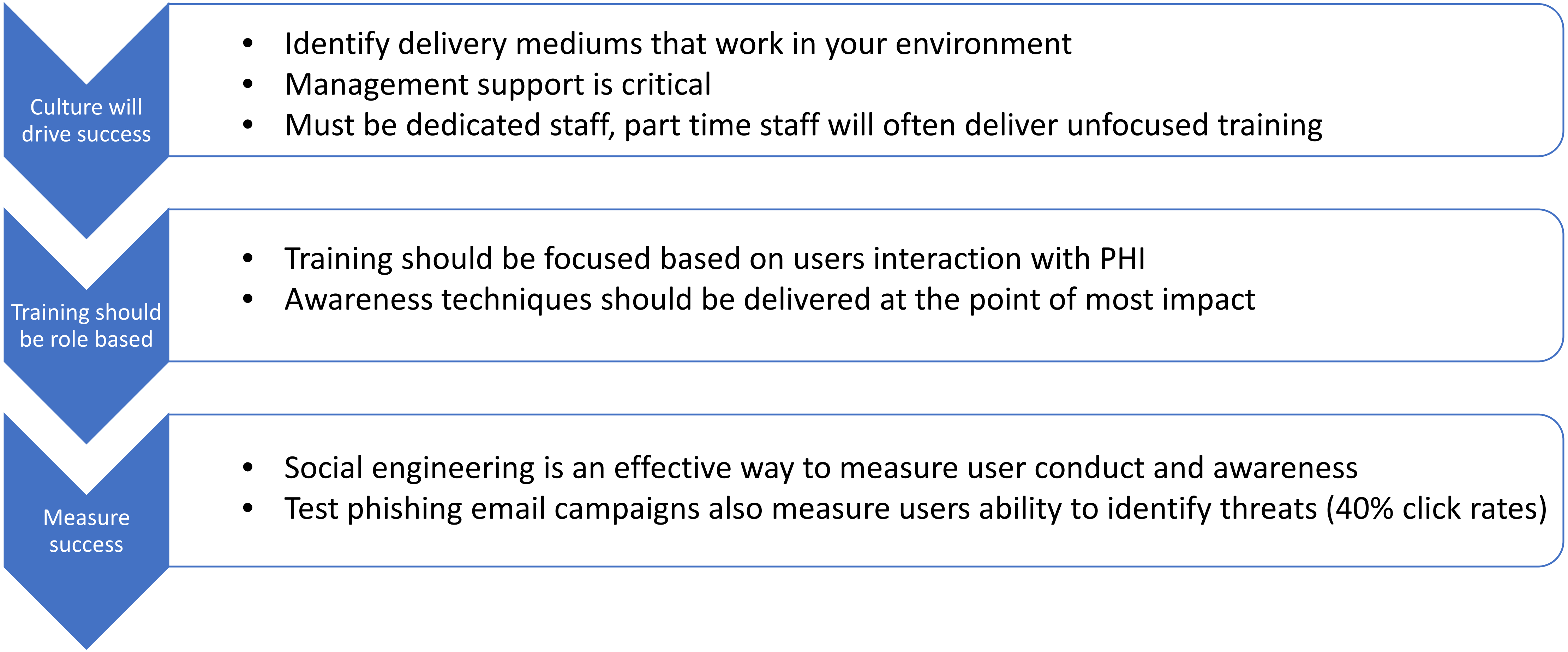
Lack of management support

Lack of resources

No explanation of *why*

Social engineering

Strategies for determining appropriate training approaches within your organization.



Culture will drive success

- Identify delivery mediums that work in your environment
- Management support is critical
- Must be dedicated staff, part time staff will often deliver unfocused training

Training should be role based

- Training should be focused based on users interaction with PHI
- Awareness techniques should be delivered at the point of most impact

Measure success

- Social engineering is an effective way to measure user conduct and awareness
- Test phishing email campaigns also measure users ability to identify threats (40% click rates)

Operationalizing training strategies

Conduct a survey of your user base to hear what training methods works for them (ISACA approach).

- What is the relationship between training frequency and perceived security effectiveness as measured by the survey?
- What is the relationship between training delivery methods and perceived security effectiveness as measured by the survey?
- What is the relationship between training compliance monitoring and perceived security effectiveness as measured by the survey?

PCI Security Standards Council - 2014

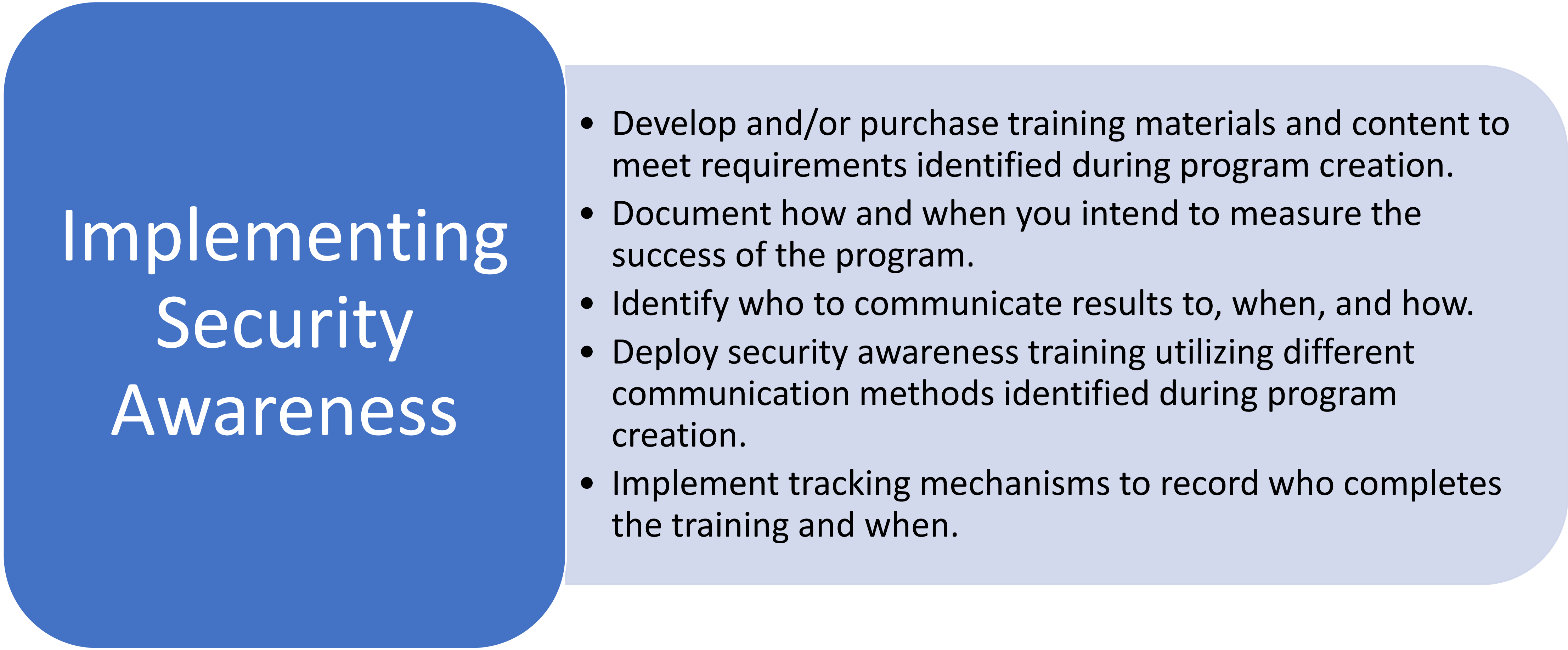
Operationalizing training strategies

Creating the Security Awareness Program

- Identify compliance or audit standards that your organization must adhere to.
- Identify security awareness requirements for those standards.
- Identify organizational goals, risks, and security policy.
- Identify stakeholders and get their support.
- Create a baseline of the organization’s security awareness.
- Create project charter to establish scope for the security awareness training program.
- Create steering committee to assist in planning, executing and maintaining the awareness program.
- Identify who you will be targeting—different roles may require different/additional training (employees, IT personnel, developers, senior leadership).
- Identify what you will communicate to the different groups (goal is shortest training possible that has the greatest impact).
- Identify how you will communicate the content—three categories of training: new, annual, and ongoing

PCI Security Standards Council - 2014

Operationalizing training strategies



Implementing Security Awareness

- Develop and/or purchase training materials and content to meet requirements identified during program creation.
- Document how and when you intend to measure the success of the program.
- Identify who to communicate results to, when, and how.
- Deploy security awareness training utilizing different communication methods identified during program creation.
- Implement tracking mechanisms to record who completes the training and when.

PCI Security Standards Council - 2014

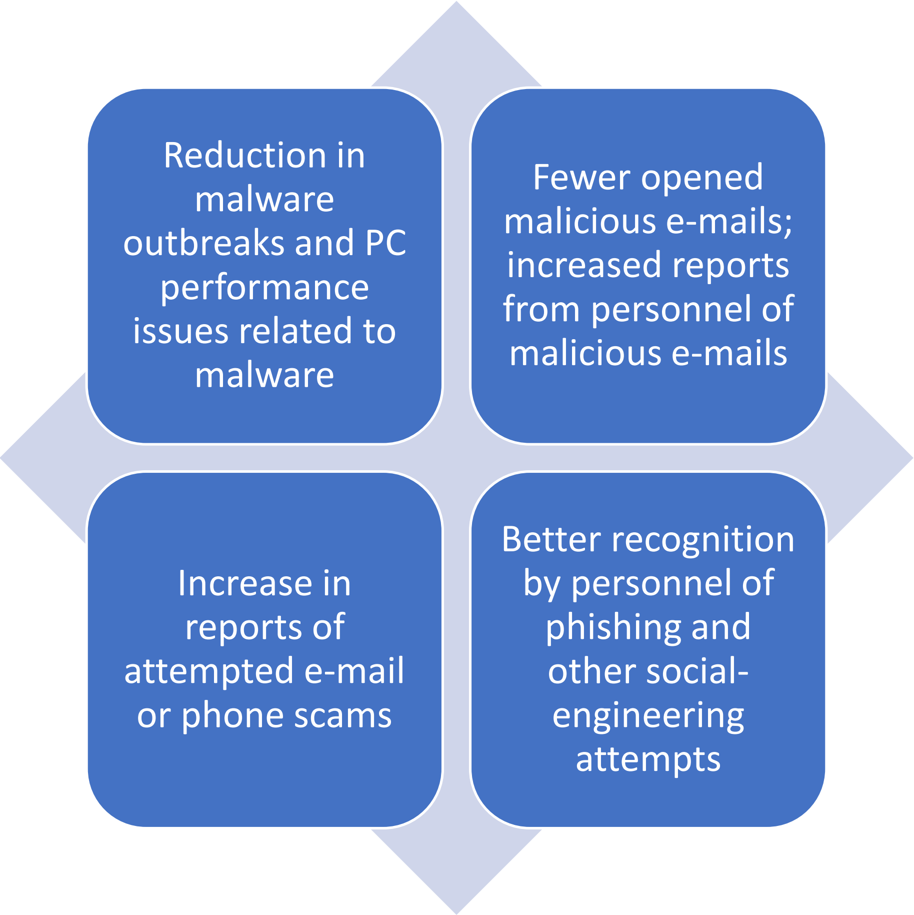
Operationalizing training strategies

Sustaining Security Awareness

- Identify when to review your security awareness program each year.
- Identify new or changing threats or compliance standards and updates needed; include in annual update.
- Conduct periodic assessments of organization security awareness and compare to baseline.
- Survey staff for feedback (usefulness, effectiveness, ease of understanding, ease of implementation, recommended changes, accessibility).
- Maintain management commitment to supporting, endorsing and promoting the program.

PCI Security Standards Council - 2014

Measuring Success (metrics)



Reduction in malware outbreaks and PC performance issues related to malware

Fewer opened malicious e-mails; increased reports from personnel of malicious e-mails

Increase in reports of attempted e-mail or phone scams

Better recognition by personnel of phishing and other social-engineering attempts

Decrease in time between detection and remediation

Increase in reporting of security concerns and unusual access

Increased understanding by personnel of risks

Increase in the number of queries from personnel on how to implement secure procedures

Q&A

Jason Griffin, CISM: Cybersecurity Practice Leader
www.orchestratehealthcare.com
jgriffin@orchestratehealthcare.com
281-221-5488 - Mobile