The Fight Against Phishing: Defining Metrics That Matter

Mark T. Chapman CFE CISSP
President and Founder

PhishLine
Measured Security Awareness

Quick Movie Reference

After being subjected to terribly boring stories for days, Steve Martin's character launches an epic rant.

> I could tolerate any insurance seminar. For days I could sit there and listen to them go on and on with a BIG smile on my face. They'd say, "How can you stand it?"
>
> I'd say, "'Cause I've been with Del Griffith. I can take ANYTHING."

Planes Trains and Automobiles
© 1987, Paramount Pictures.

Rest assured, if this presentation goes as expected, you will be unbelievably prepared for ANYTHING at your next seminar!

PhishLine
Measured Security Awareness

The Fight Against Phishing

The most damaging information security attacks often use low-tech social-engineering methods to trick users into sharing sensitive information. In spite of the significant money spent on email and web content filtering technologies, organizations ultimately must rely on the generally unreliable “human firewall” to thwart phishing attempts. For such an important class of critical security controls, **it is surprisingly rare to formally configure and manage the human layer beyond ad-hoc techniques based on anecdotal, incomplete and inaccurate information.**

There are now ways to safely use some of the methods employed by attackers to provide objective, understandable and **actionable metrics** to proactively measure, manage and improve the effectiveness of the last line of defense.

PhishLine
Measured Security Awareness

Defining Metrics That Matter

They must be:

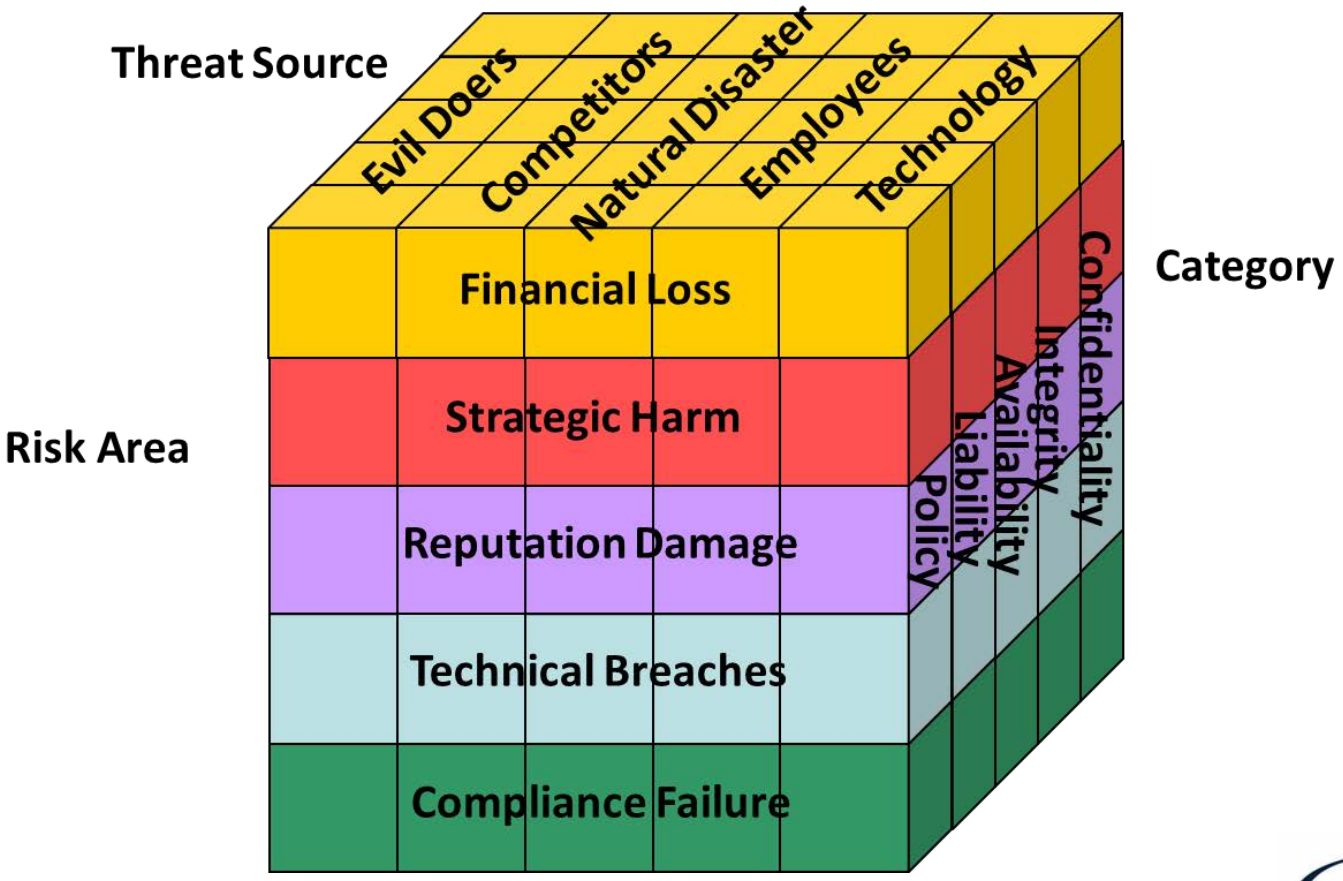
- **Contextual**
- **Relevant**
- **Actionable**

Are we speeding? It depends on context.
School Zone? Slow down!
Race Track? Speed up!

PhishLine
Measured Security Awareness

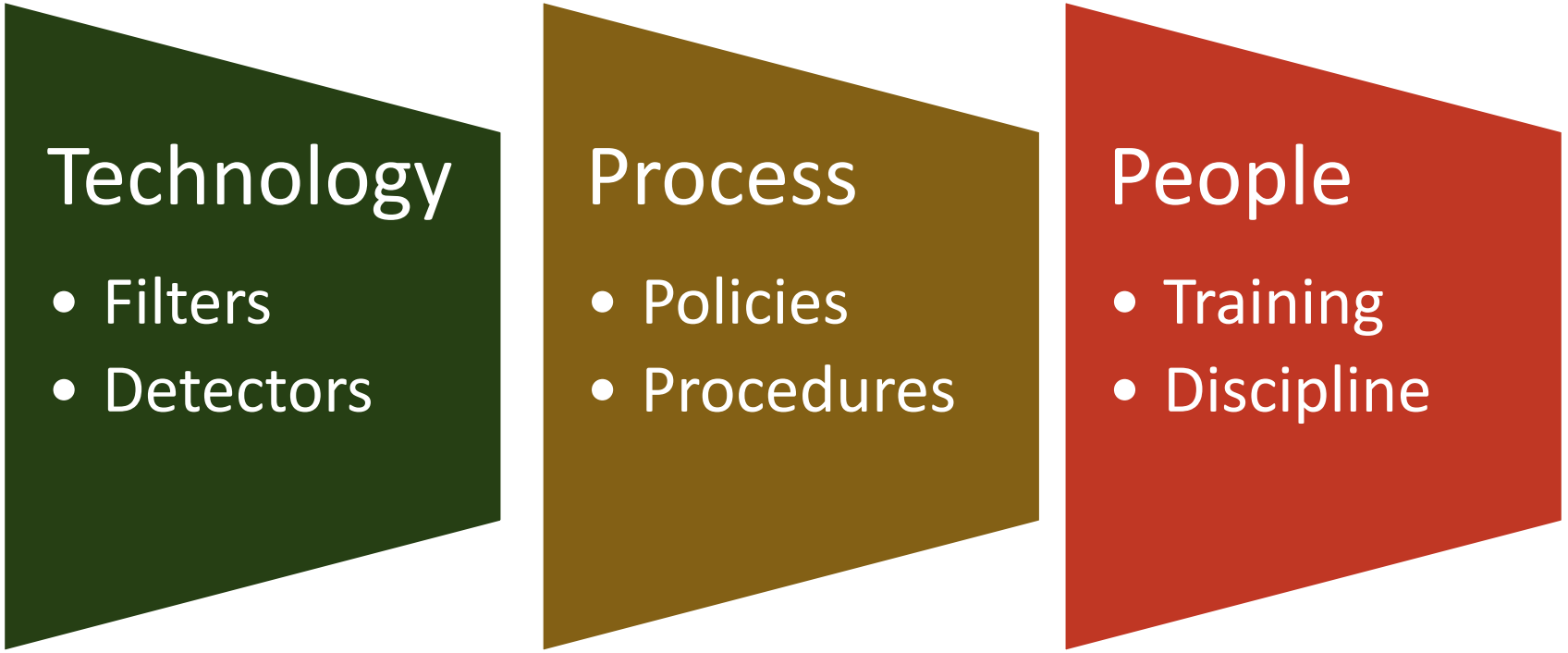
Which Metrics Matter to the Enterprise?

Can there be ”too much” context?



PhishLine
Measured Security Awareness

How Does An Enterprise Mitigate Risk?

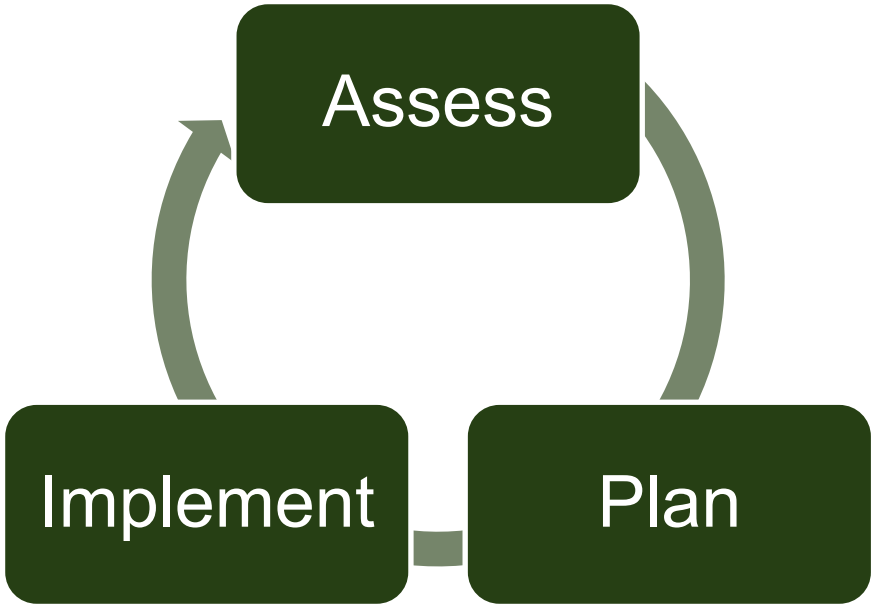


PhishLine
Measured Security Awareness

Technology Risk Management

Technology

- Filters
- Detectors



PhishLine
Measured Security Awareness

Technology Risk Management

Technology

- Filters
- Detectors

White-Box Testing

- Code reviews / configuration audits.

Black-Box Testing

- Vulnerability/penetration testing.

Reporting & Metrics

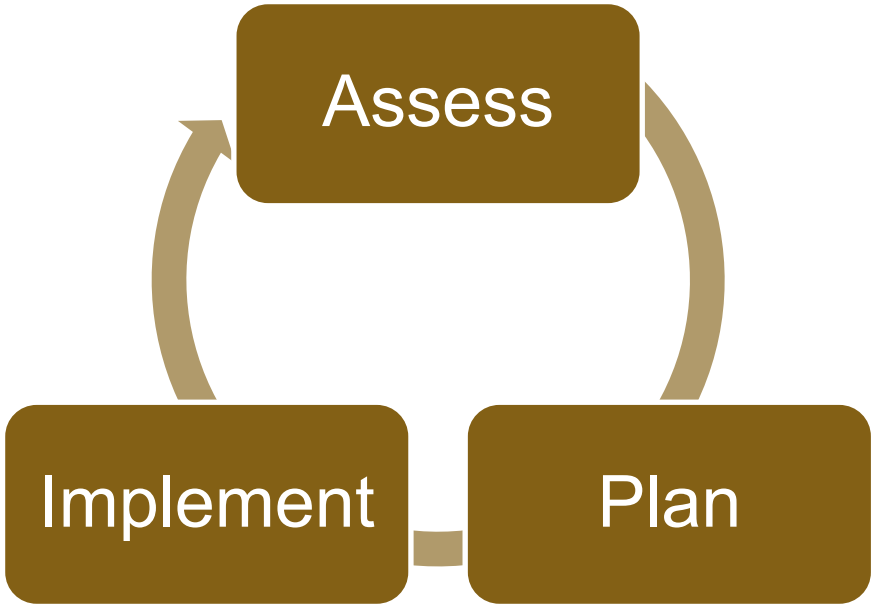
- What are some actionable metrics?

PhishLine
Measured Security Awareness

Process Risk Management

Process

- Policies
- Procedures



PhishLine
Measured Security Awareness

Process Risk Management

Process

- Policies
- Procedures

White-Box Testing

- Compliance / Regulatory reviews

Black-Box Testing

- Audit using sampling techniques

Reporting & Metrics

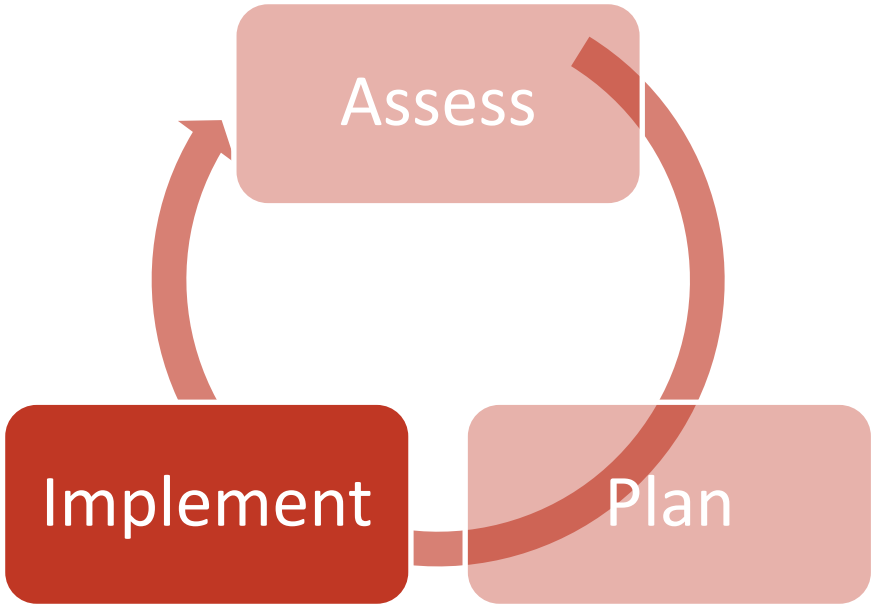
- What are some actionable metrics?

PhishLine
Measured Security Awareness

Human Firewall Risk Management

People

- Training
- Discipline



PhishLine
Measured Security Awareness

Human Firewall Risk Management

People

- Training
- Discipline

White-Box Testing

- Security awareness training with post testing

Black-Box Testing

- Social engineering attack simulations

Reporting & Metrics

- What are some actionable metrics?

PhishLine
Measured Security Awareness

Criteria For Actionable Metrics

Contextual

Relevant

Actionable

- **GOOD METRICS DRIVE GOOD RESULTS.**
- **THE BEST METRICS DRIVE THE BEST RESULTS.**
- They are clear, understandable and relevant.
- They provide on-going visibility at multiple levels.

PhishLine
Measured Security Awareness

Share Understandable Security Metrics and Trends

- How many people replied to a suspicious email?
- How many users clicked on a website link or attachment?
- How many entered data into a web form?
- How does this trend compare to prior campaigns?
- How does this compare to benchmarks?

PhishLine
Measured Security Awareness

Plan

People

- Training
- Discipline

Define Objectives

- What are you trying to accomplish?

Leverage Actionable Metrics

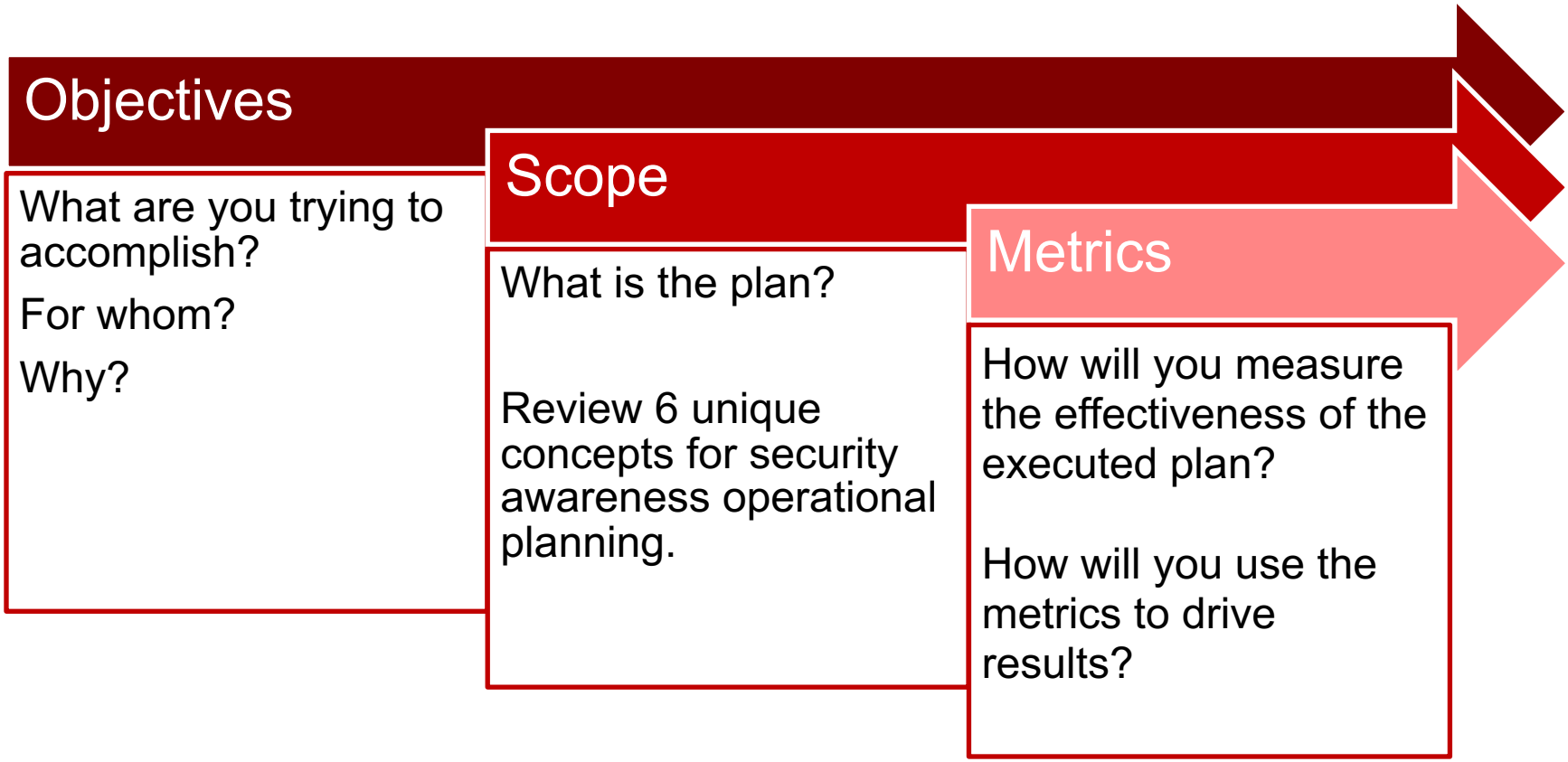
- Specific, actionable assessment metrics.

Finalize Plan Details

- A complete plan cannot be perfect.

PhishLine
Measured Security Awareness

Information Security Awareness Operational Planning



PhishLine
Measured Security Awareness

Objectives

What are the goals?

1. List objective statements.
2. Identify stakeholders.
3. Capture the "why".

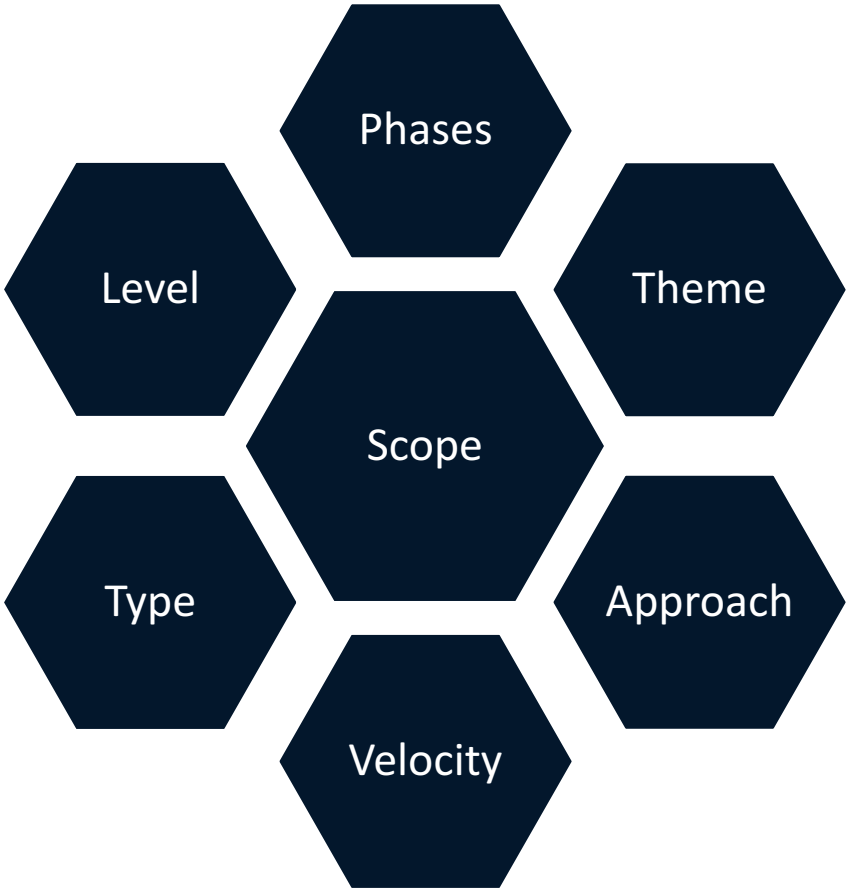
"Initially, we want to create a baseline for phishing vulnerability assessments to enable future remediation."

"We want to test the effectiveness of our annual security awareness training."

"We want to find out what time of day our employees are most susceptible to phishing attacks."

PhishLine
Measured Security Awareness

Scope



- An Information Security Awareness Operational Plan includes all the standard components of any good risk-based project plan, such as resources, budgets and timelines.
- It also includes specific curriculum targets.
- There are six unique concepts related to information security awareness programs.

PhishLine
Measured Security Awareness

Scope

Phases

- One-time audit
- Baseline testing
- Annual training
- Targeted training
- Advanced Persistent Testing

Story: Mobile Device Security Targeted Training

PhishLine
Measured Security Awareness

Scope

Theme

- Basic spam.
- Recent general phishing threats.
- Industry-specific phishing attacks.
- Organization-specific spear-phishing.
- Learning science principals.

Story: Company Picnic Registration

PhishLine
Measured Security Awareness

Scope

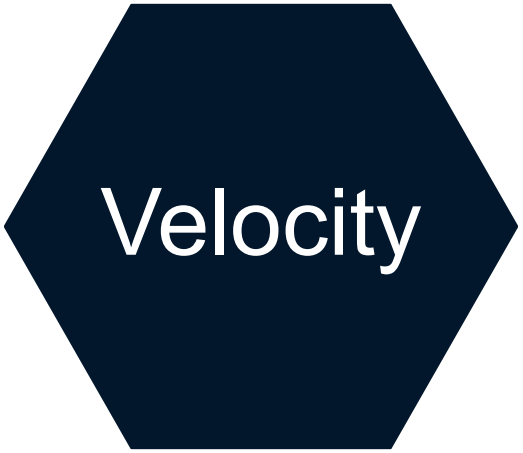
Approach

- Blind vs. Informed.
- It depends on:
  - Corporate culture.
  - How you will use the results to effect change.

Story: Metrics as Security Awareness Training

PhishLine
Measured Security Awareness

Scope

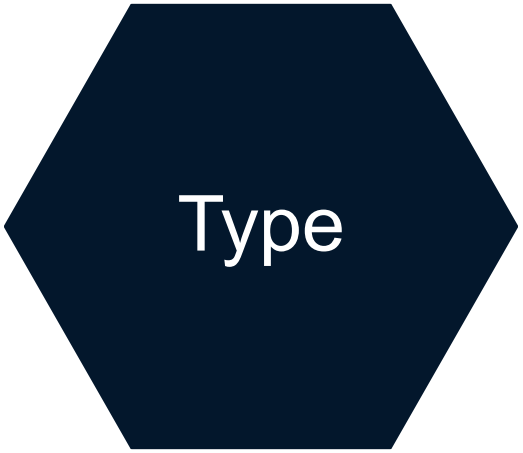


- Low & Slow vs. Blitz.
- Advanced Persistent Threats vs. Swift Attack.

Story: “Gopher” network

PhishLine
Measured Security Awareness

Scope



- Email campaigns.
- Portable media campaigns.
- Text/smishing campaigns.
- Voice/vishing campaigns.
- Snail-mail campaigns.

Story: Portable Media Mahem

PhishLine
Measured Security Awareness

Scope

Level

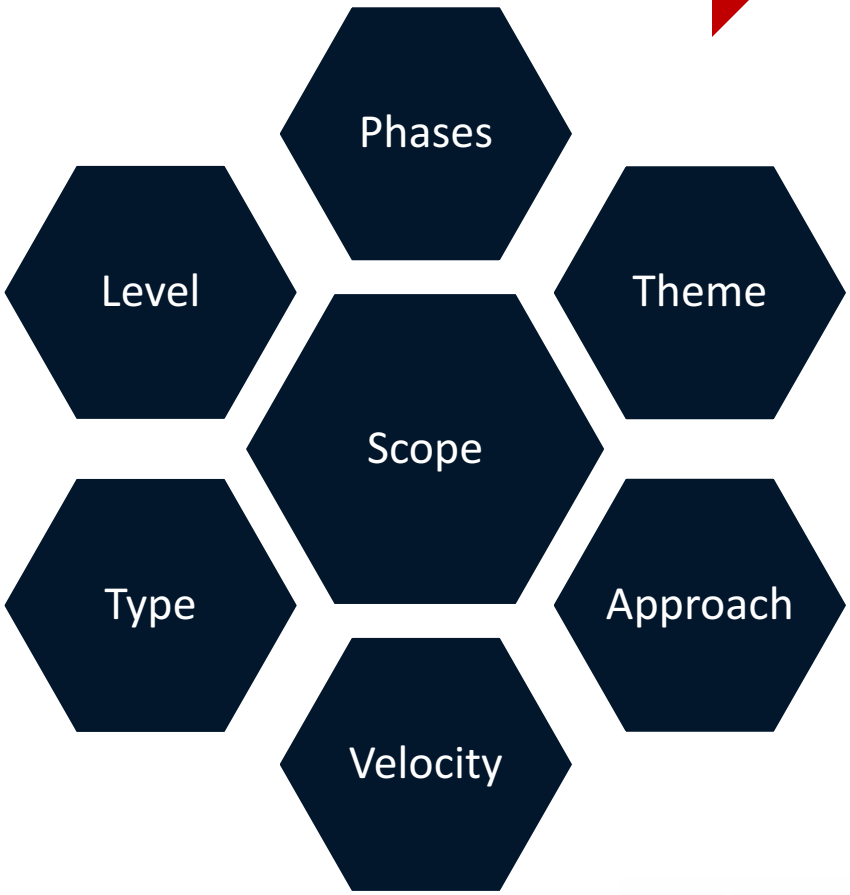
- The level of difficulty.
- How “genuine” should the messages be?
- Use real logos and convincing names?
- Use inside information?
- Start low and go high for maximum leverage.

Story: “PupilSoft” Captcha

PhishLine
Measured Security Awareness

Scope

- An Information Security Awareness Operational Plan should integrate with the good risk management work done in related areas.
- The purpose of the six key concepts is to add granularity to actionable metrics and corresponding actions to improve your organization's security posture.



PhishLine
Measured Security Awareness

Take Away - Checkpoint

1. Leverage what you already know about Technology and Process Risk Management to address the Human Layer.

2. Implement a risk-based Information Security Awareness Operational Plan that fits your organization.

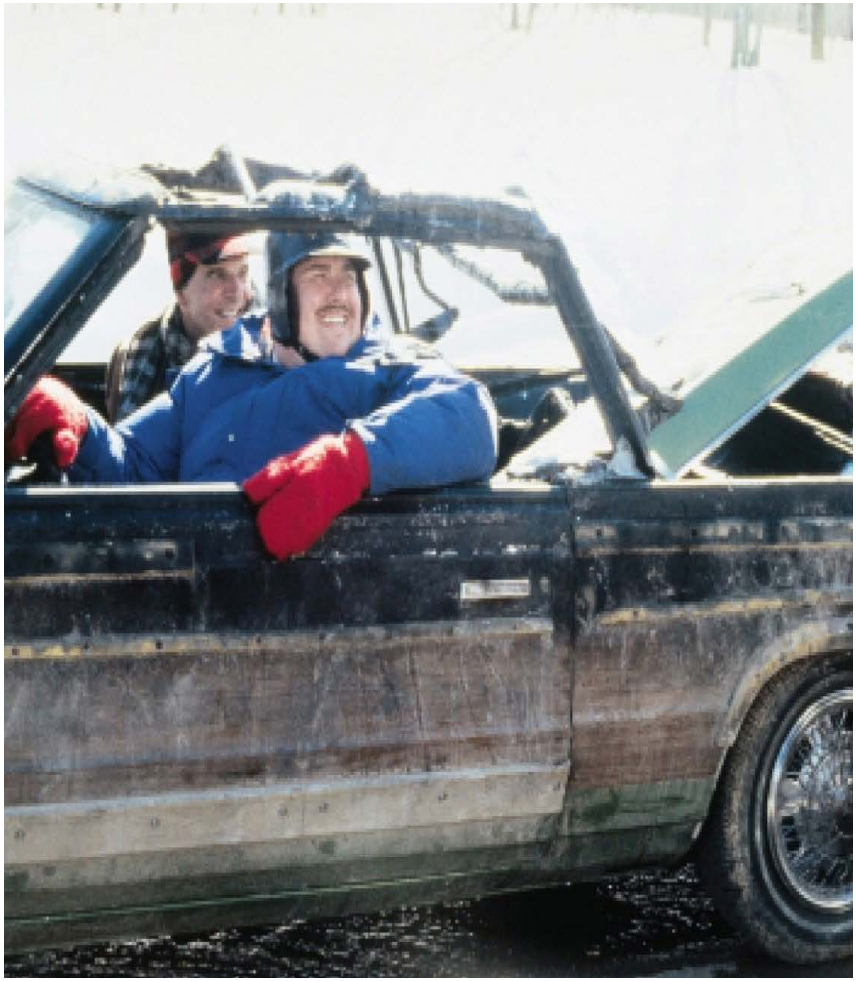
3. Perform objective tests, such as mock phishing campaigns, to measure, manage and reinforce key awareness concepts.

4. Start at a basic level and work your way up to a more complex Advanced Persistent Testing ecosystem.

5. Use actionable metrics to literally TAKE ACTION and drive the Plan -> Implement -> Assess cycle.

PhishLine
Measured Security Awareness

THANK YOU!!!



PhishLine
Measured Security Awareness

Contact Information

Mark T. Chapman, CFE CISSP
President and Founder, PhishLine, LLC.
mchapman@phishline.com

PhishLine
Measured Security Awareness