



**Study Results:
Failure-Triggered Training Trumps Traditional Training**

Sean Palka

Booz | Allen | Hamilton

delivering results that endure



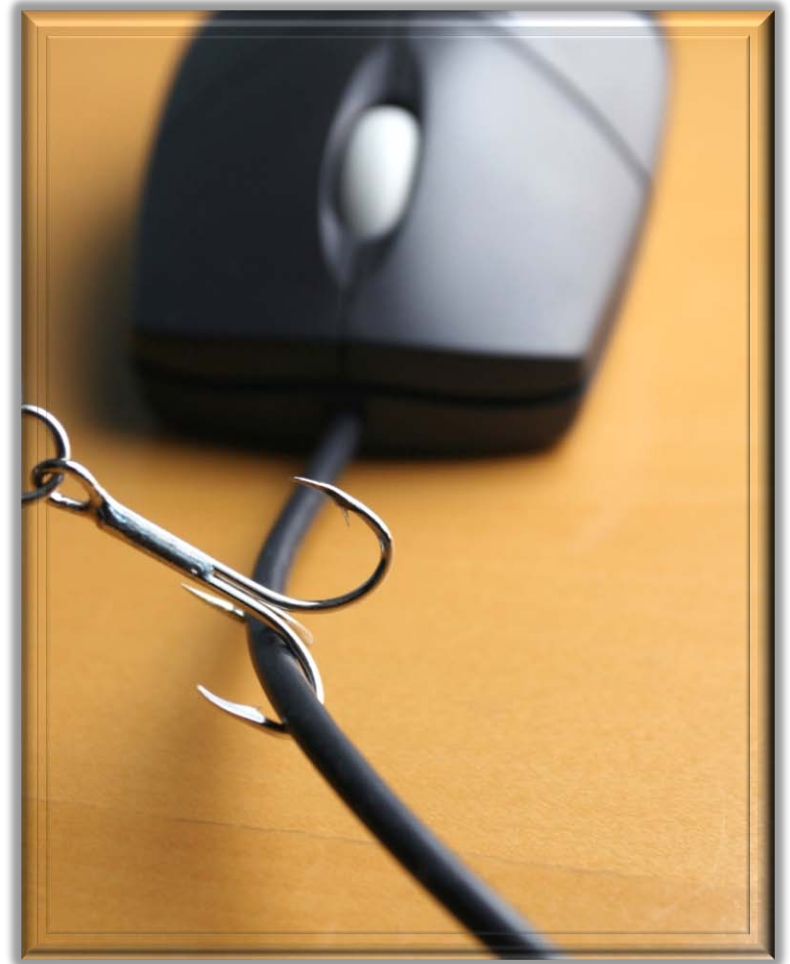
Sean Palka
palka_sean@bah.com

Booz | Allen | Hamilton

delivering results that endure

Social Engineering Attacks Impact You and Your Organization by . . .

- Wasting fiscal resources
- Increasing costs
- Damaging reputations
- Causing clients to lose trust or go elsewhere





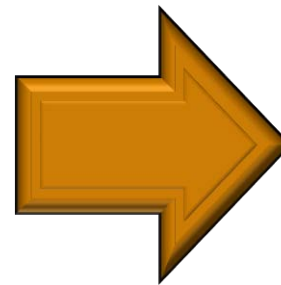
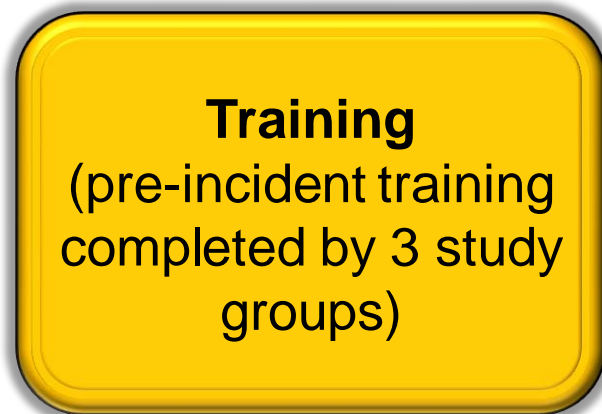
“Phishing attacks” target the weakest link in the information security chain — the individual end users. These attacks are really a **people problem first** and a technology problem second.

Our Study Sought to Determine if . . .

- Interactive phishing awareness training would
 - Be significantly more effective for learning transfer than both placebo and static page-turning training
 - Receive satisfactory reaction ratings and post-test scores
- Failure-triggered training would have a significant positive impact on learning transfer

Failure-triggered training: Unannounced blind exercises delivered in spaced intervals, combined with immediate tailored remedial training provided only to the users that “fail” the exercises.

After Initial Training, Groups Received Unannounced Attacks Over a 9-Month Period



Post-Training Reaction Survey
(Kirkpatrick Evaluation Level 1 reaction data)

Training Post-Test
(Kirkpatrick Evaluation Level 2 learning data)

Failure-Triggered Training
(Kirkpatrick Evaluation Level 3 behavior data)

Control Group Received: Placebo Training

Control Group training **did not** address how to respond to phishing attacks



The lessons of past eras reveal five main principles for developing a viable cyber strategy:

- Invest in all three sectors of society—government, business and civil society—so that cyber's enabling capabilities are widely shared and balanced over the long term.
- Build trust and confidence in cyberspace so that organizations and people will take full advantage of cyber's capabilities.
- Address issues of cyber enablement and cybersecurity as joint problems, recognizing that they are interconnected pillars of cyberpower.
- Promote broad and collaborative engagement among stakeholders from all sectors, geographic regions, and levels of government.
- Adopt a comprehensive approach that enables stakeholders to collaborate in addressing shared, multidimensional cyber problems.

Experimental Group 1 Received: Traditional Static Training

Web-based Attacks



Experimental Group 1 training included phishing awareness content copied from a wiki

victim into submitting their personal information. Once at the website, the attacker must continue to trick the victim into believing that personal information is required. The websites are often carbon copies of the real sites having similar fonts and images.

Web-based attacks are categorized into the following classes:

- Fake Banner Advertising Attacks
- Man-in-the-Middle Attacks
- URL Obfuscation Attacks
- Cross Site Scripting (CSS or XSS) Attacks

Experimental Group 2: Received Interactive Training

Experimental Group 2 training included “**identifying suspicious item**” activities to enable the practice of proper action responses

ONLINE
Phishing Revealed

You clicked a link in an e-mail that tried to access a suspicious external website. Suspicious sites may try to steal your personal information or install a virus. E-mails and instant messages can be modified to appear to be coming from a trusted source, instead of the attacker.

How to protect yourself:

Rollover each icon to read more.

Forward, as an attachment, suspicious e-mails to
CIRT
(BAH Corporate Incident Response Team)

The next page will TEST your understanding of phishing by identifying suspicious features in suspicious e-mails.

Inbox - Microsoft Outlook

From: IT [t345@bah.com]

Message Developer

Contracts_Su
Contract Support
Dear John Smith:
IT [t345@bah.com]
Change your pas
Morton [pro
Re: Virus
A recent sweep of

Subject: Change your password

Date: 8 July, 2010

It is mandatory for you to change your password. We're sorry for the trouble but it is important to protect you. You will be asked for your name, current password, date of birth, and social security number. Your supervisor will be notified if this is not completed within 24 hours.













http://password_manager.booz&allen&Hamilton.com.tw

Attempts Remaining:
1

Phrases Remaining:
3

VERIFY STATEMENT

Study Results Show Highest Reaction Ratings for Interactive and Wiki Training

	Overall Assessment	Delivery was engaging	I am better prepared to recognize phishing	I would recommend to others (Yes)
Control Group (N=114)	 3.4	 3.5	 2.7	 63%
Wiki Group (N=88)	 3.7	 3.6	 4.1	 85%
Interactive Group (N=114)	 3.8	 4.1	 3.9	 85%

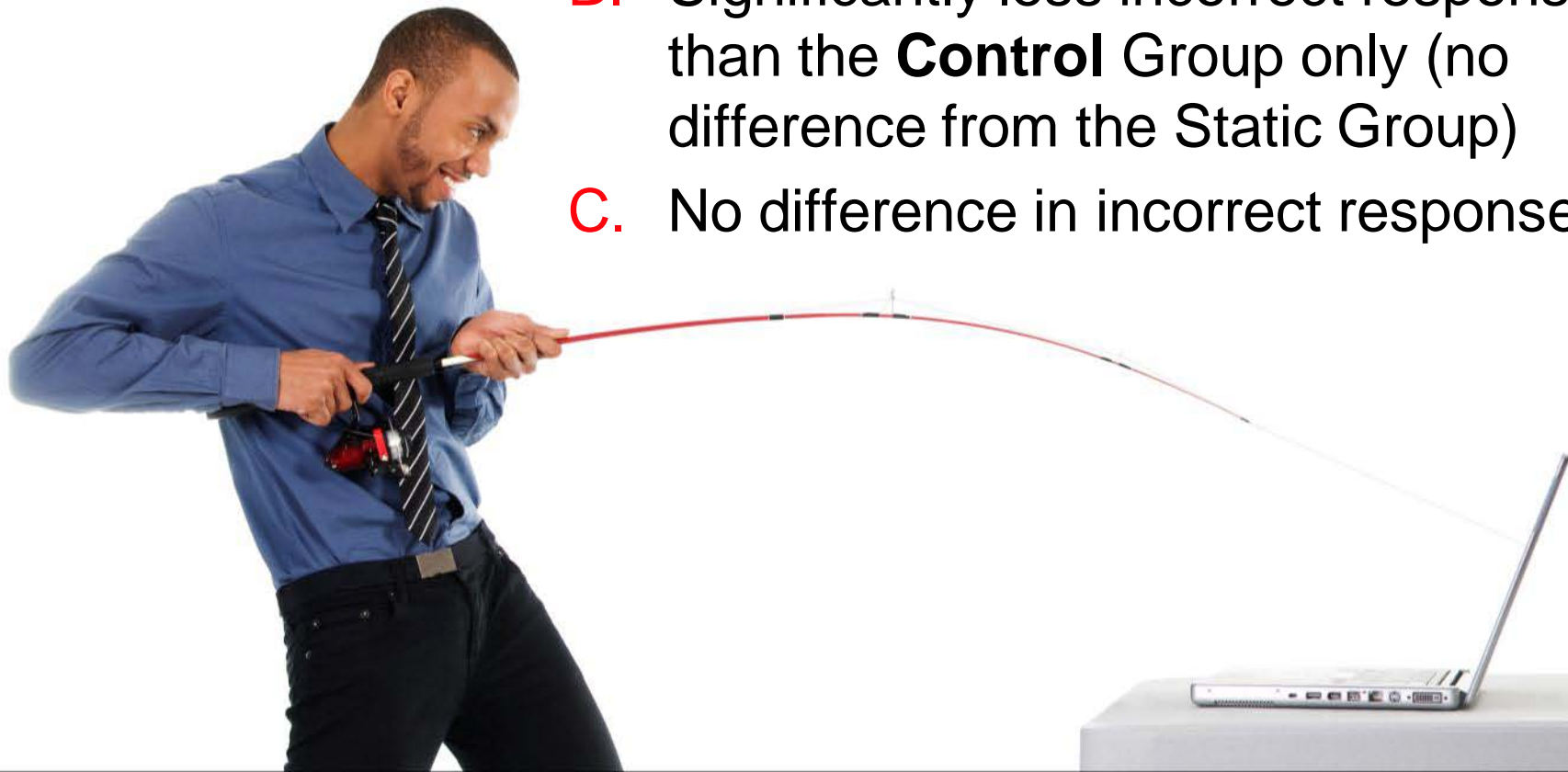
Maximum score 5.0

Post-Tests Indicated Both Experimental Groups Knew How to Respond to Suspicious Emails

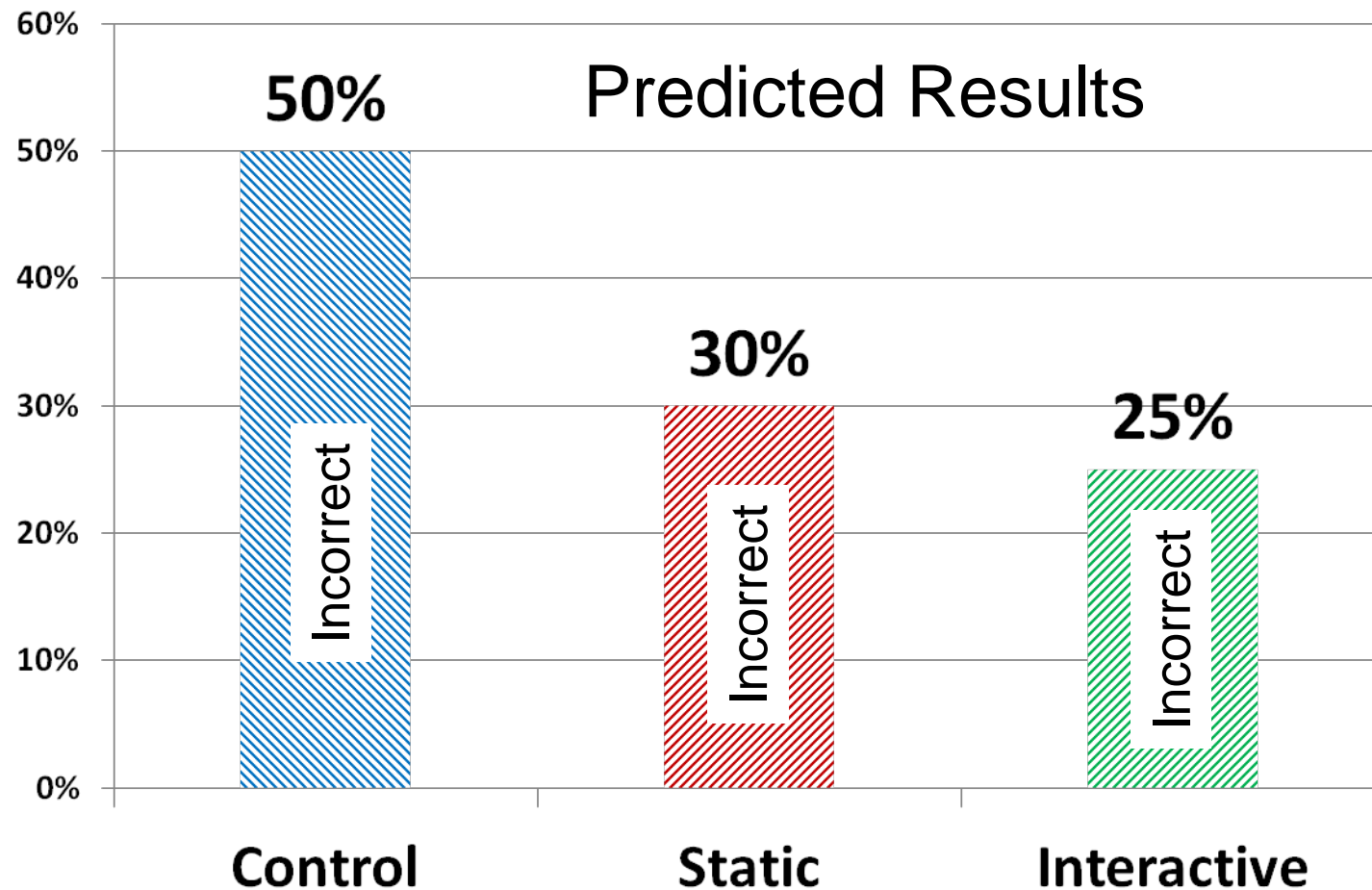
	Correct Response to: Who should be notified of suspicious emails
Wiki Group (N=88)	87.8%
Interactive Group (N=114)	95.6%

When simulated phishing attacks are sent, the use of interactive training will result in

- A. Significantly less incorrect responses compared to **both** the **Control** and **Static** groups
- B. Significantly less incorrect responses than the **Control** Group only (no difference from the Static Group)
- C. No difference in incorrect responses

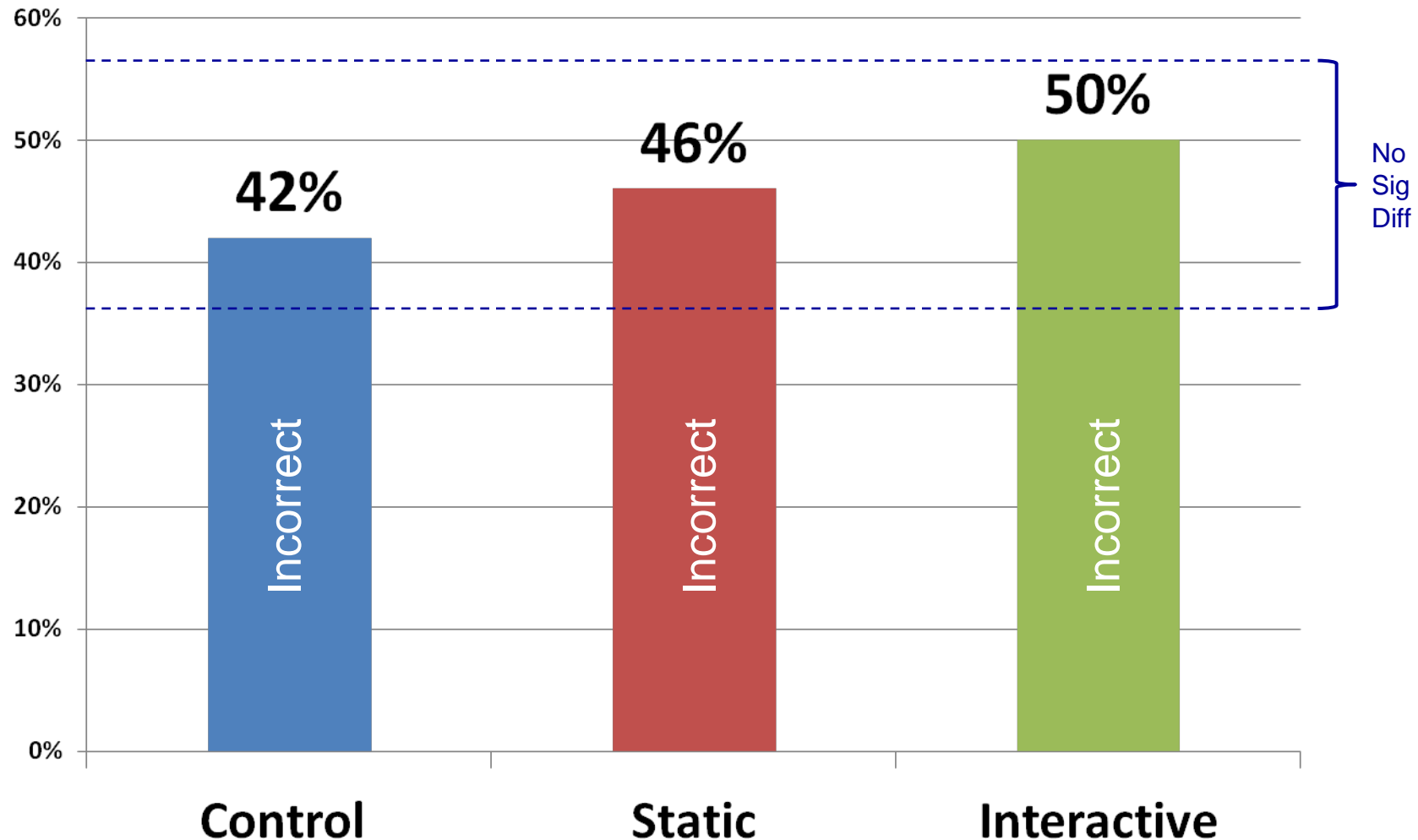


What We Expected . . .



Following training, we conducted unannounced simulated attacks. We expected to have **significantly more incorrect actions** from the Control Group than the Experimental Groups.

What We Discovered in Exercise 1 . . .



Based on the simulated attacks, we discovered
no significant difference between training and no training!

What Do You Do When Training Fails (WTF)?



We Used Failure-Triggered Training



Failure-Triggered Training is like the “Secret Shoppers” used by the retail shopping industry.

Over the Next Six Months, Study Participants Received Three Exercises

Participants were sent three different phishing emails on spaced intervals. Each user's response/action was tracked.

Correct Responses

Incorrect Responses



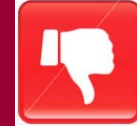
User deletes the email (no responses are captured)



User reports the email through appropriate channels



User clicks an inappropriate link in the email

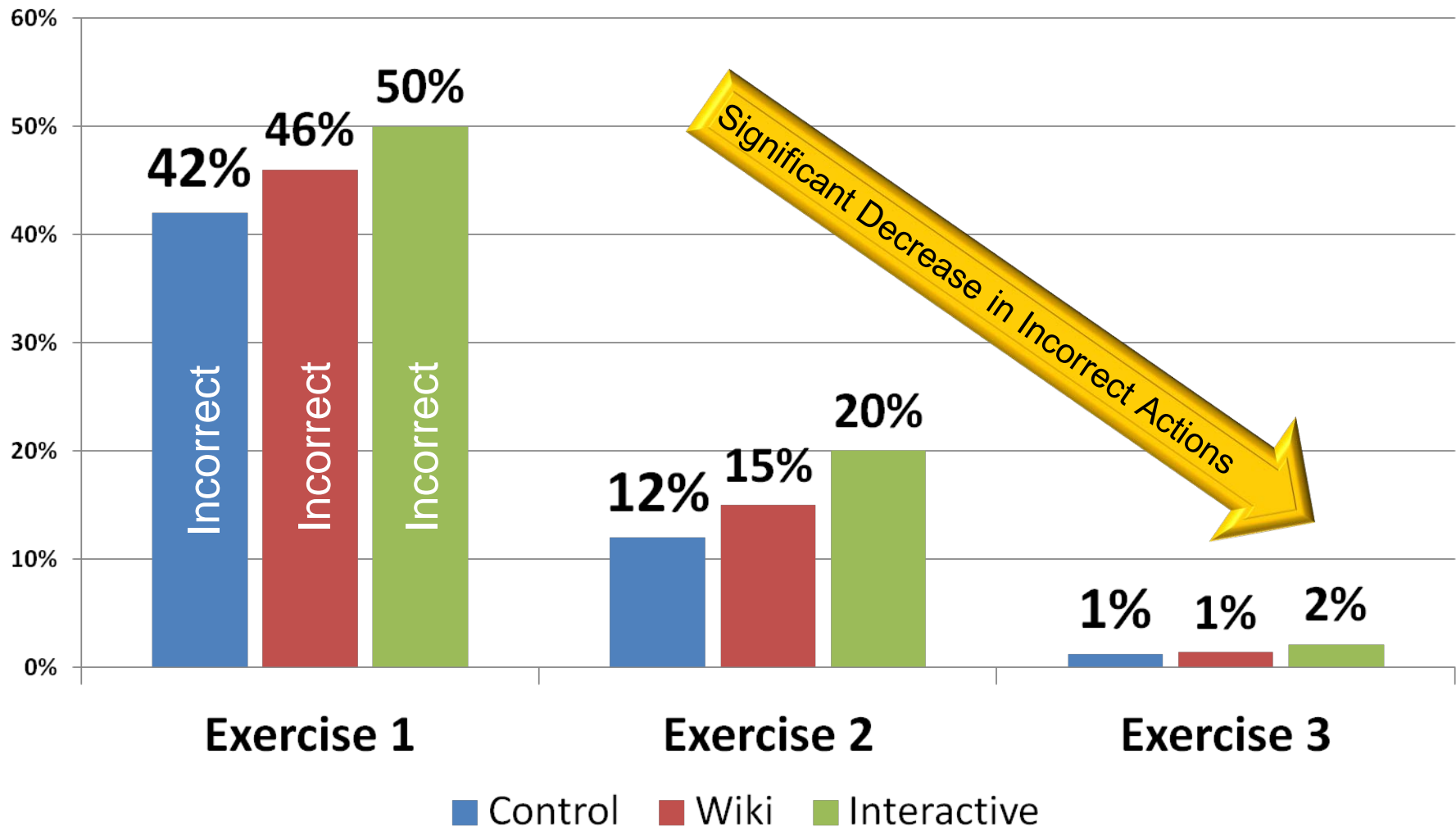


User directly responds to the email

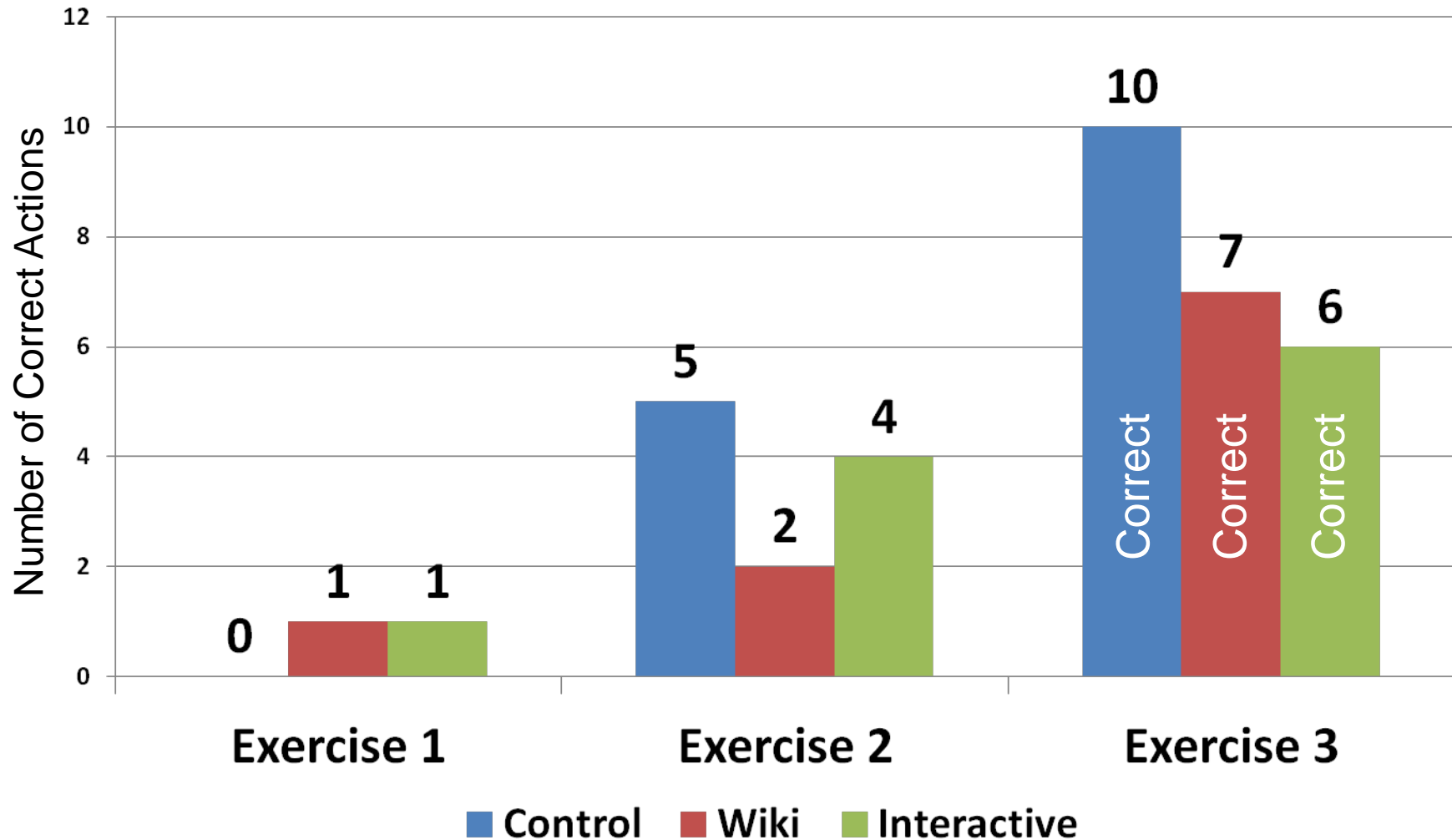


- Failure-triggered training is delivered
- Response metrics aggregated using the STAR*Phish™ system

Study Results Show Incorrect Responses Decreased Significantly ($P < 0.05$) Between Each of the Exercises Over a Period of Months



Study Results: The Number of Reports to CIRT (AKA - An Additional Correct Action) Increased with the Failure Triggered Training Approach

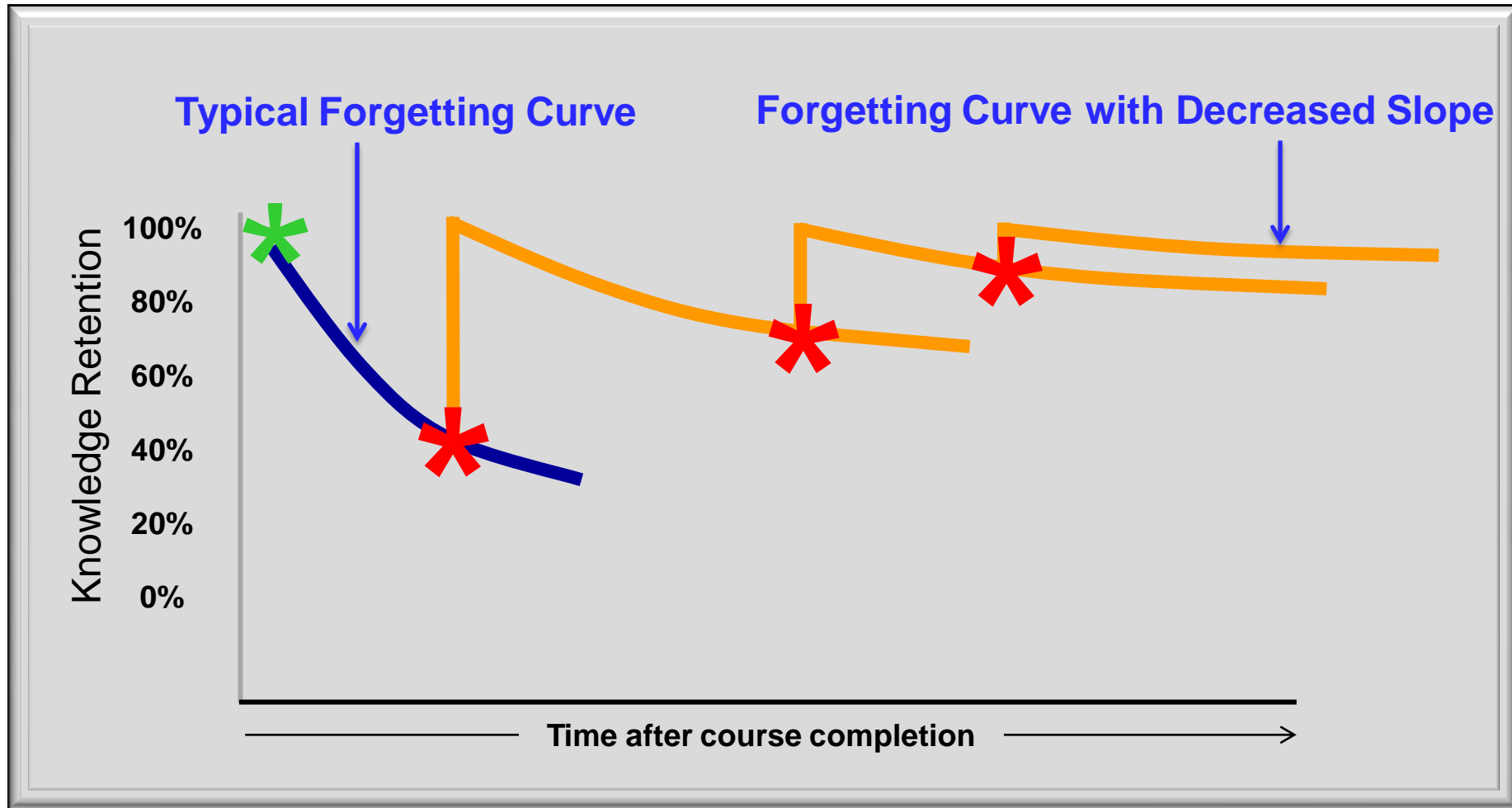


Learning at the point of realization refers to the state when users are open to learning because **relevance**, **knowledge gaps**, and **immediate needs** are identified in an **engaging/unexpected** and **concrete** fashion.



The phishing training seems to have triggered a point of realization for the learners.

Spaced Learning Effect and Forgetting Curve



✱ Learning Event ✱ Failure-Triggered Training Event

Quote from a study participant that correctly reported an external phishing attack to the Critical Incident Response Team (CIRT) highlights that learning at the point of realization may greatly influence the level of learning transfer.

“I learned about the CIRT team through the phishing training email sent out a couple months back. It really stuck with me, since I ‘failed the test.’”

Remember, Our Study Sought to Determine if . . .

- Interactive phishing awareness training would
 - Receive satisfactory reaction ratings and post-test scores
 - **CONFIRMED**
 - Be significantly more effective for learning transfer than both placebo and static page training
 - **NOT CONFIRMED**
- Failure-triggered training would have a significant positive impact on learning transfer
 - **INDICATED**

What We Learned Was . . .

- Traditional one-time, pre-incident training was ineffective
- Failure-triggered training resulted in a positive significant difference
- Reaction to an actual external phishing attack indicated knowledge transfer
- Multiple training elements may have to be present for successful learning transfer

Failure-triggered training: Unannounced blind exercises delivered in spaced intervals, combined with immediate tailored remedial training provided only to the users that “fail” the exercises.

Follow-On Questions and Next Steps

- How much impact does the email content have on the results?
- How important was the interactivity level of the failure-triggered training?
- Do users respond to emails and failure-triggered training differently on mobile devices?