



Critical Considerations when Choosing a Security Awareness Training Vendor

How Do You Set Yourself and Your Organization Up for Success?



Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.



Perry Carpenter
Chief Evangelist & Strategy
Officer

About Perry

- MSIA, C|CISO
- Author of *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors*
- Former Gartner Analyst leading research and advisory services to CISOs, Security Leaders, and security vendors around the world
- Led security initiatives at Fidelity Information Services, Alltel Telecommunications, and Wal-Mart Stores
- Lover of all things:
 - Security
 - Psychology
 - Behavioral Economics
 - Communication Theory
 - Magic, misdirection, and influence

About KnowBe4



- The world's most popular integrated new-school Security Awareness Training and Simulated Phishing platform with tens of thousands of customers around the world
- Founded in 2010
- Recognized as a Leader in the Gartner Magic Quadrant for Computer-Based Training (CBT)
- Our mission is to train your employees to make smarter security decisions so you can create a human firewall as an effective last line of defense when all security software fails...

Which it will

A security culture lives and breathes within every organization.

The question is how **strong, intentional** and **sustainable** is your security culture. And **what do you need to do about it?**

Agenda

- What should organizations consider when planning a security awareness program?
- Where can vendors help?
- What makes KnowBe4 unique?

Agenda

- What should organizations consider when planning a security awareness program?
- Where can vendors help?
- What makes KnowBe4 unique?

**Security
Awareness:
because...
well, you
know**



-- a harsh reality --

Traditional awareness programs **fail** to account for
the *knowledge-intention-behavior gap*...

MIND THE GAP

We need to *condition people* to have the *right reflexive behaviors*



**“Everybody has a plan
until they get punched
in the mouth.”
- Mike Tyson**

There are *Three Realities* of *Security Awareness*



1

Just because I'm **aware** doesn't mean that I **care**.

2

If you try to work **against** human nature, you will **fail**.

3

What your employees **do** is way more important than what they **know**.

Thinking, Fast & Slow (Daniel Kahneman)



THE 2 SYSTEMS



READINGGRAPHICS
ACTIONABLE INSIGHTS IN ONE PAGE

System 1 (Fast Thinking)

Continuously scans
our environment.



Fast but error-prone



Works automatically
& effortlessly via
shortcuts, impulses
and intuition.



System 2 (Slow Thinking)

Used for specific
problems, **only if
necessary**



Takes effort to analyze,
reason, solve complex
problems, **exercise
self-control**



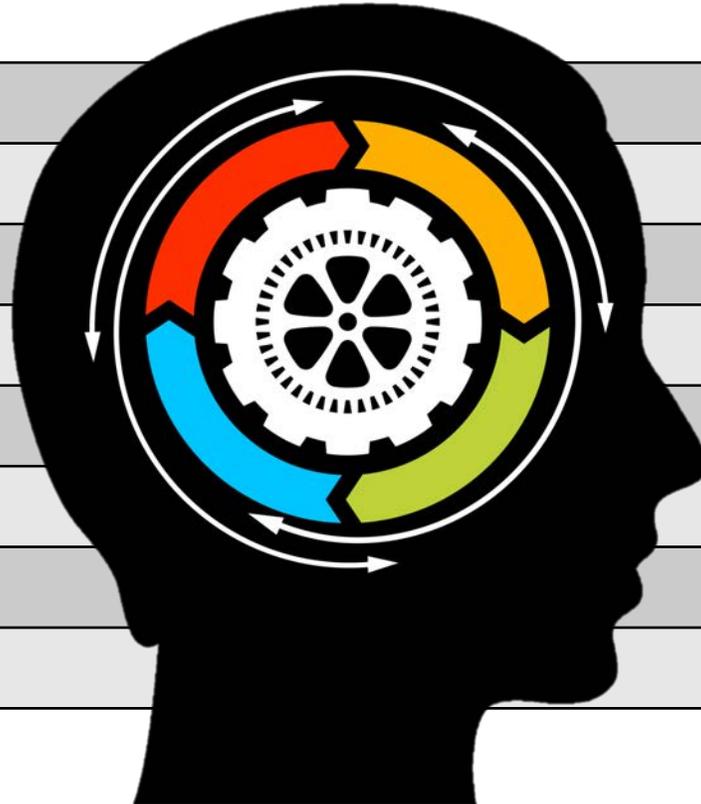
Slow but reliable



A Person Is Actually Part of a Broad Ecosystem

Thought and behavior are influenced by:

World Views	Observed Behavior of Executives
Regional Context	Known and Perceived Expectations
Peer Groups	Knowing or Feeling That They Are Watched
Culture in Their Division	Subliminal Influence
Previous Experiences	Systems of Reward and Reprimand
Pressures at Home	Social Currency and Social Pressure
Pressures at Work	Ambitions
Patterns of Habit	Fears



Agenda

- What should organizations consider when planning a security awareness program?
- Where can vendors help?
- What makes KnowBe4 unique?

Critical Components of a Security Awareness Training Program



Content



Executive Support & Planning



Campaign Support Materials



Testing



Metrics & Reporting



Surveys/Assessments

-- a sobering truth --

Your **awareness program** and **content** are the **visible 'face'** of your department to the **rest of your company.**

70:20:10 Model for Learning and Development



70% EXPERIENCIAL

On-the-job, social, in the workflow, corporate and departmental culture

20% INFORMAL

Asking others, collaborating, watching videos, reading

10% FORMAL

Structured learning, LMS courses, training days

70:20:10 Model for Learning and Development

Most companies spend 90% of their efforts on the 10%.



Create/find content to use across the whole 100%.

The Five Moments of Need

1. For the first time
2. Wanting to learn more

Point in time,
Just in case

3. Trying to apply knowledge and/or remember
4. When something goes wrong
5. When something changes

Just in time



Think about
Learner Profiles/Segments
Where Possible

You need powerful ways to split your user population into groups. This allows you to measure them and train them in ways that best resonate with their individual needs and learning styles.

Why Is Getting the Desired Behaviors So Difficult?



BJ Fogg
@bjfogg

 Follow

3 truths about human nature: We're lazy, social, and creatures of habit. Design products for this reality.

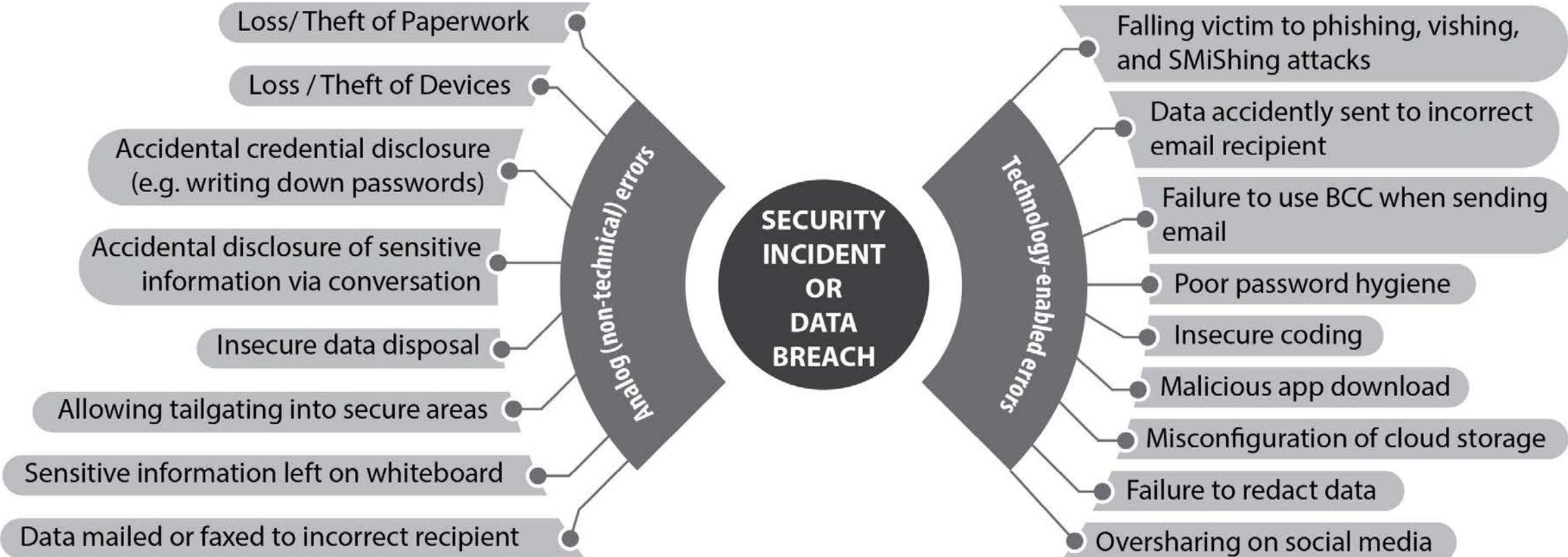
<http://bit.ly/bjfoggcamp>

10:59 AM - 31 Mar 2011

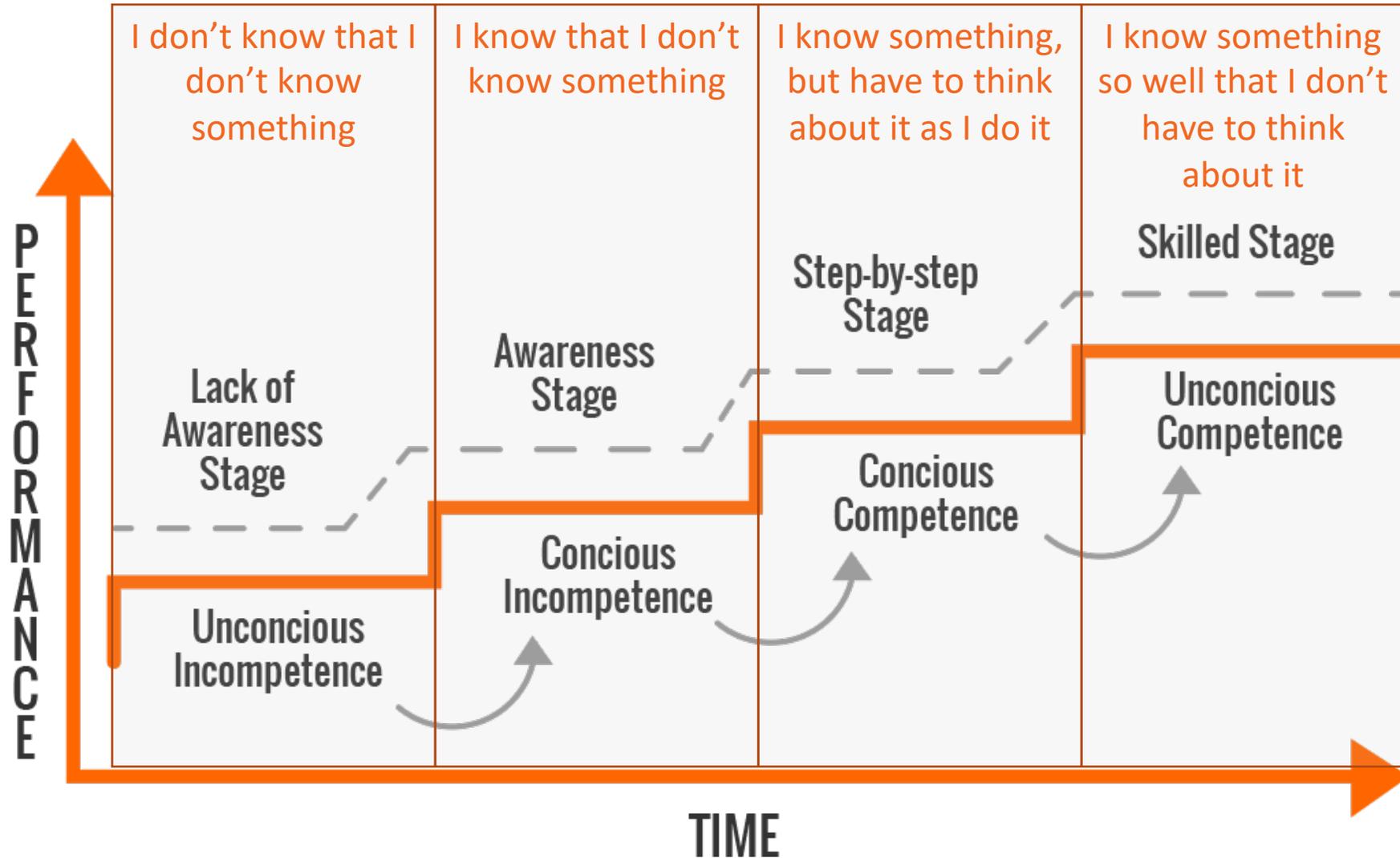
  24  15



Remember that Not All Incidents are Techno-centric

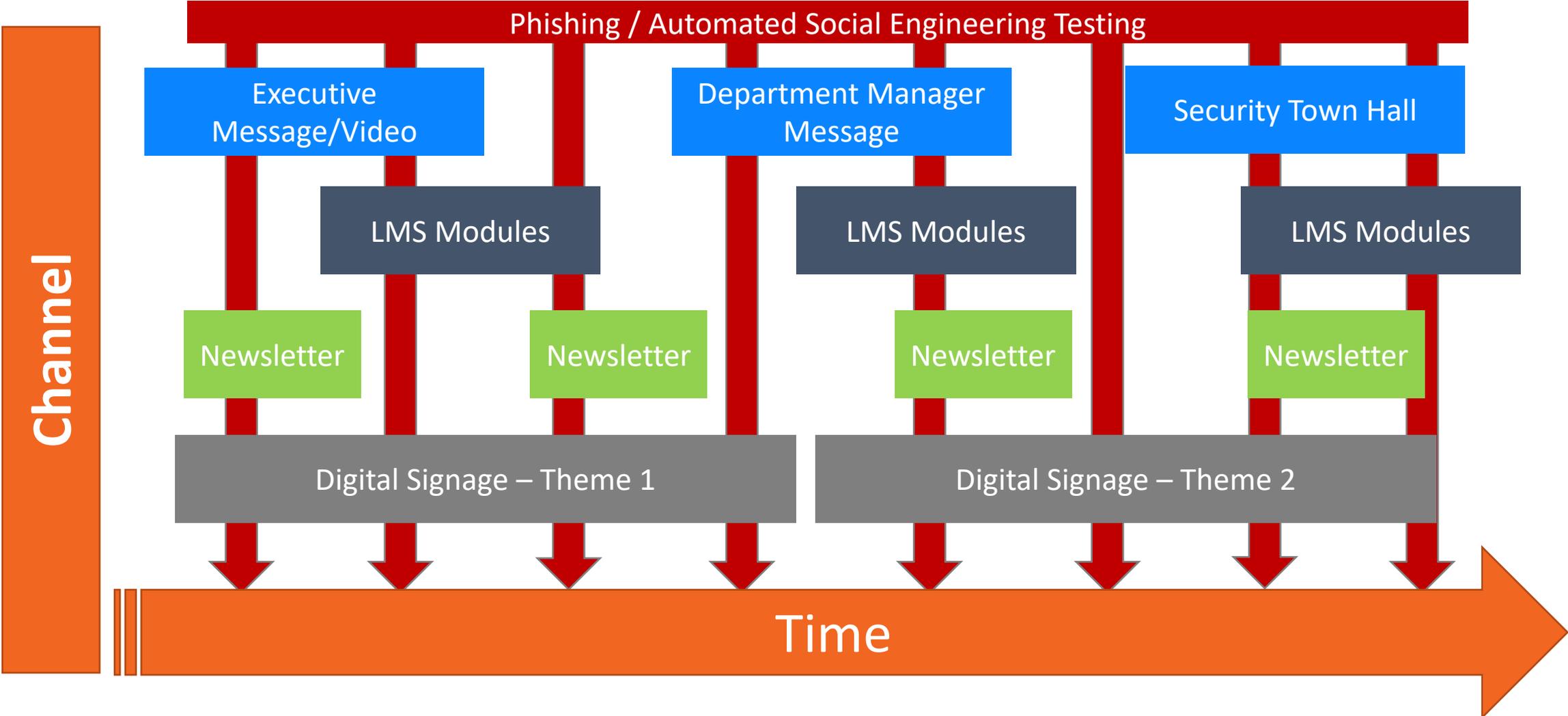


The Four Stages of Competence



Noel Burch, Gordon Training International, Conscious Competence Ladder – 1970s

Plan like a Marketer. Test like an Attacker.



Agenda

- What should organizations consider when planning a security awareness program?
- Where can vendors help?
- What makes KnowBe4 unique?

The following are two slides I created
about the security awareness market
in **early 2017**.

Future trends:

- **Flexible and adaptive:** Greater context-awareness and real-time intervention
- **Focus on time savings:** micro-learning, behavioral baselining, test-outs, fine-grained roles/rules
- **Smarter:** Broader use of AI and machine learning
- **Plug-able:** More integrations with 'traditional' security tools



Future trends:

- **Sneakier**: Broader automated social engineering use cases
- **Sensitive**: Learner sensitive and aware
- **More flavorful**: More variety of content, styles, tones, formats, etc...
- **Assistive**: Will naturally encourage greater program maturity

Those “Future Trends” are now current
reality at KnowBe4.

With over 30,000 customers (and growing), nearly 1,000 employees, and offices in 9 countries, KnowBe4 is the world's most-popular and most proven security awareness vendor.

Customers *love* KnowBe4!

- 1,340 total Gartner Peer Insights reviews: that's more than all reviews vendors from the 2019 MQ Vendors combined.
- 1,060 **Five-Star** Gartner Peer Insights reviews.
- Winner of Gartner Peer Insights Customer Choice Awards for Security Awareness CBT Category
- Winner of Frost & Sullivan Global Cyber Security Awareness Training Platform Company of the Year
- Consistently mentioned in analyst-user roundtables as a most-loved security vendor



Data as of November 2019

Unsurpassed Thought Leadership



Kevin Mitnick
Chief Hacking Officer



Perry Carpenter
Chief Evangelist &
Strategy Officer



Roger Grimes
Data-Driven Defense
Evangelist



Javvad Malik
Security Awareness
Advocate



Kai Roer
CLTRe Founder
Security Culture Advocate



Joanna Huisman
SVP Strategic Insights &
Research



Jim Shields
Founder, Twist & Shout.
Creative Director



Rosa Smothers
SVP Cyber Operations



Winn Schwartau
Founder, Security Awareness
Company

No other vendor in this market can touch the depth and breadth of KnowBe4's thought leadership... period.

Platform for Awareness Training and Testing



- 1 Phish Your Users
- 2 Train Your Users
- 3 See the Results

Creative Tools For Impactful Phishing Campaigns

The screenshot displays the KnowBe4 Account Admin interface. At the top, it says "This is the Account Admin View" and "Click here to go back to Reseller control panel". The main header includes the KnowBe4 logo and navigation tabs for "DASHBOARD" and "PHISHING".

The central focus is an "Email Preview - Wire Transfer" window. The email details are as follows:

- From:** Office of the CEO <ceo@kb4-demo.com>
- Reply-to:** ceo.gpnps.preview-mode@knowbe4.employeeportal.net-login.com
- Subject:** Wire Transfer
- Attachment:** WIRING INSTRUCTIONS.pdf

The email body contains the following text:

Hi Aaron,

Please process a payment of \$34,295 (USD) to the account information attached. Code it as an Admin expense and let me know when it is completed. Please do this as soon as possible. It is urgent.

Thanks,

Office of the CEO
ceo@kb4-demo.com

Below the email preview is a configuration form for the campaign. The form includes fields for:

- Name:** Wire Transfer (Spoofs Domain)
- Sender's Email Address:** ceo@[domain]
- Sender's Name:** Office of the CEO
- Reply-To Email Address:** ceo@[domain]
- Reply-To Name:** Office of the CEO
- Subject:** Wire Transfer
- Attachment filename:** WIRING INSTRUCTIONS

Each of these fields has a red flag icon and the text "add a red flag" below it, indicating a security warning. A callout box highlights the "Sender's Email Address" field, showing a detailed view of the field with the placeholder "ceo@[domain]" and the "add a red flag" warning.

In the background, the "Phishing Security" dashboard is visible, showing a campaign named "CEO Fraud Test" with 540 recipients and 540 delivered. A table at the bottom lists recipients, including Fritz Connell, with a scheduled time of 03/28/2018 01:42 AM.

Easy-to-Integrate, Built to Scale for Organizations of All Sizes

<input type="checkbox"/>	Full Name	Email Address	Phish Prone%	Group
<input type="checkbox"/>	Aaron Anderson	[Redacted]	0.0%	IT, Accounting, Production, Sales
<input type="checkbox"/>	Abigail Langosh	[Redacted]	12.5%	kb4-demo.com, Production, SG Midwest Clickers, TEST
<input type="checkbox"/>	Ai Windler	Ai.Windler@[Redacted]-demo.com	0.0%	kb4-demo.com, Production



<input type="checkbox"/>	Full Name	Email Address	Phish Prone%	Group
<input type="checkbox"/>	Aaron Anderson	[Redacted]	0.0%	IT, Accounting, Production, Sales
<input type="checkbox"/>	Abigail Langosh	[Redacted]	12.5%	kb4-demo.com, Production, SG Midwest Clickers, TEST
<input type="checkbox"/>	Ai Windler	Ai.Windler@[Redacted]	0.0%	kb4-demo.com, Production West

Robust Insights and Visualization Capabilities

Organization's Risk Score



See our [Virtual Risk Officer \(VRO\) Guide](#) for details about how Risk Scores are calculated.

Risk Score Factors

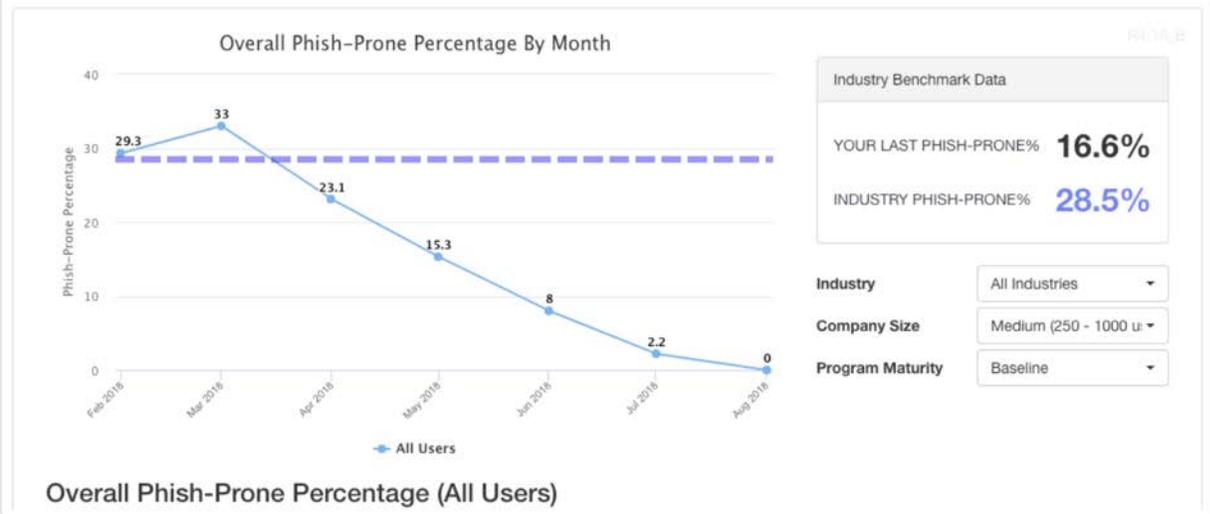
08/10/2018



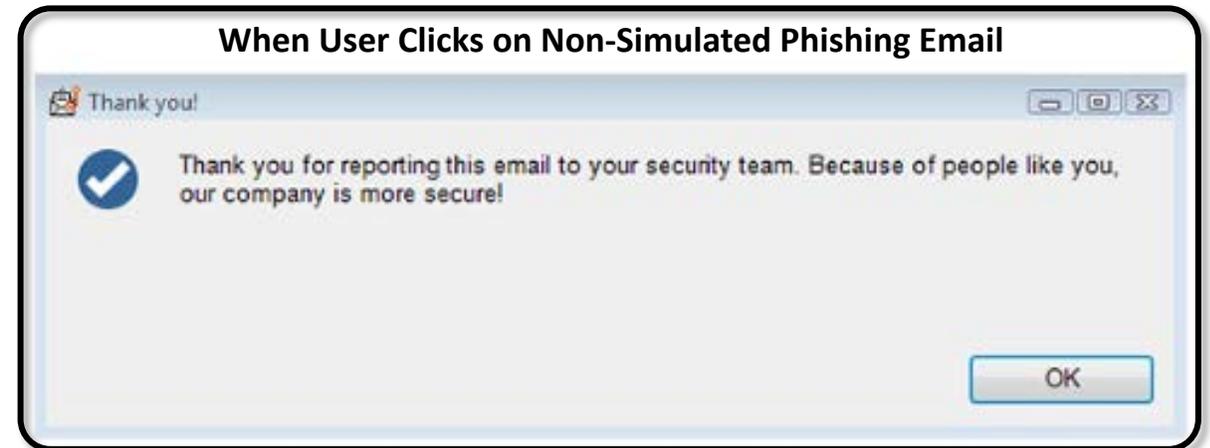
Phish-Prone Percentage ?

Reporting On: Group By: User Groups:

Date Range:



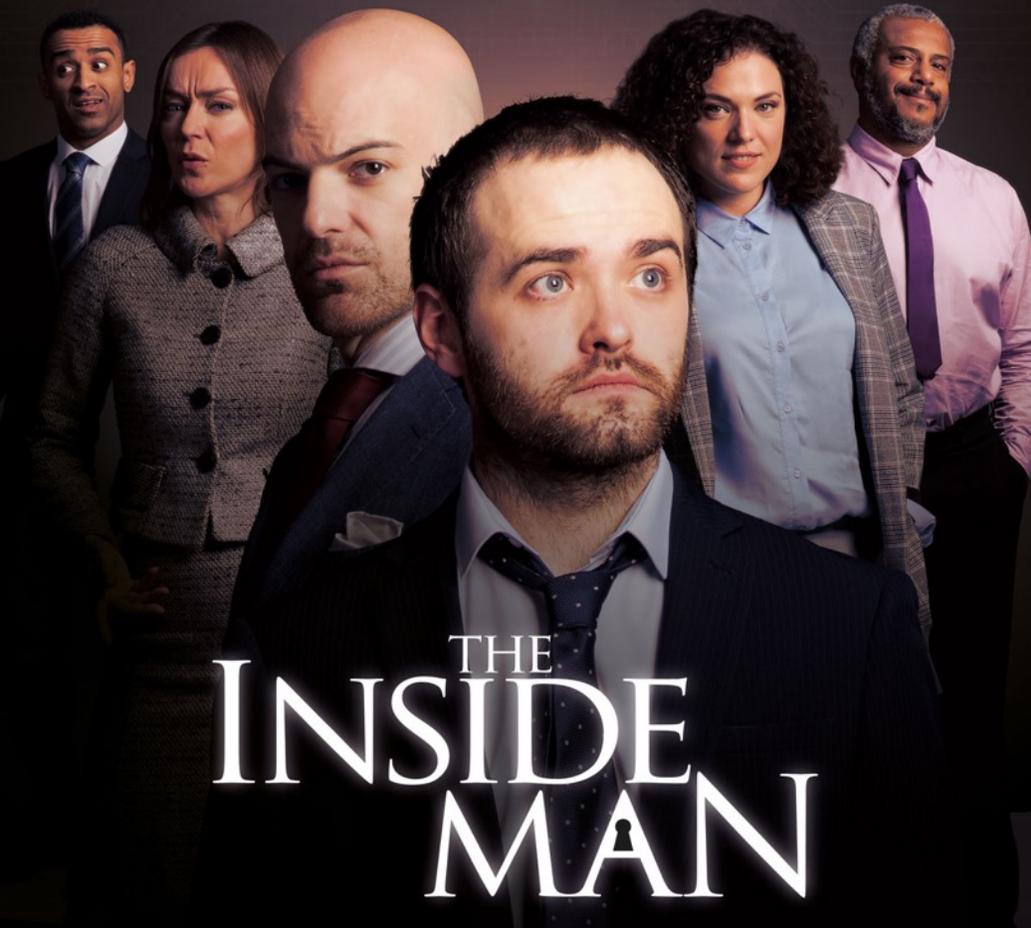
Security Liabilities Will Become Security Assets



- Increase User Engagement
- Reduce Phishing Prone Percentage
- Empower Your Response Team

Reinforce Your Security Culture with Employee Training

FAKE LIFE.
REAL CONSEQUENCES.



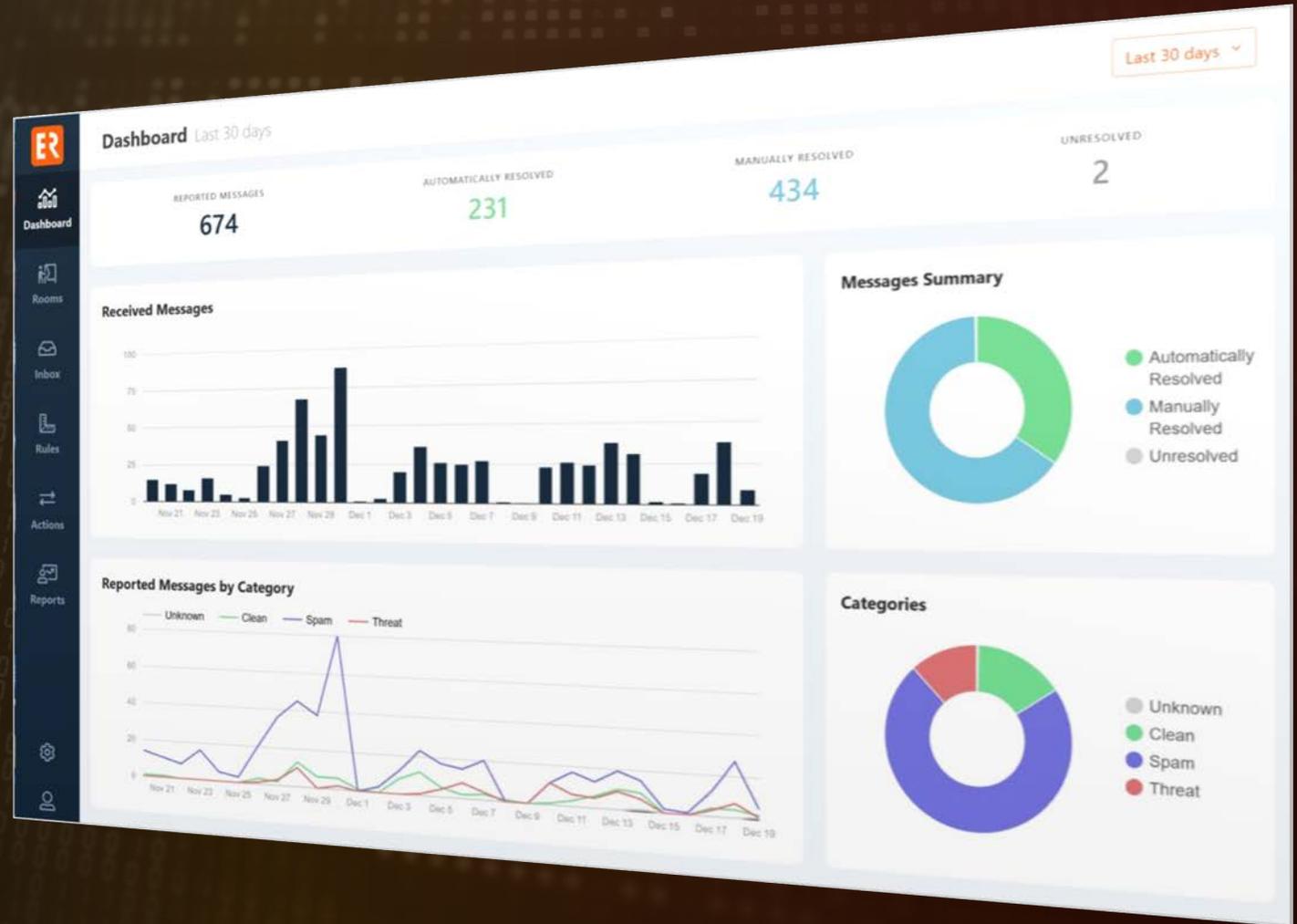
THE INSIDE MAN

COMING SOON
TO A DESKTOP NEAR YOU.

New-school Awareness Training



- ✓ Automatic processing using custom rules
- ✓ Send to external sources (Virus Total, SIEM, etc.)
- ✓ Automated disposition
- ✓ Automated feedback loop to employees
- ✓ Prioritize message for human attention
- ✓ Fewer security resources required to manage email threats



A hand is shown placing a puzzle piece into a larger puzzle piece that forms a person's silhouette. The background is a blurred image of a person in a white shirt. The text "Security Awareness Doesn't Have to be Hard" is overlaid in white.

Security Awareness Doesn't Have to be Hard



Thank You

KnowBe4
Human error. Conquered.

Perry Carpenter, MSIA, C|CISO

Chief Evangelist & Strategy Officer

Email: perry@knowbe4.com

Twitter: [@PerryCarpenter](https://twitter.com/PerryCarpenter)

LinkedIn: [/in/PerryCarpenter](https://www.linkedin.com/in/PerryCarpenter)