

The Next Evolution of Security Awareness

Awareness, Behavior, Culture, & Human Risk



Perry Carpenter
Chief Evangelist &
Strategy Officer KnowBe4, Inc.



Kai Roer
Chief Research Officer
KnowBe4, Inc.

got culture?

In November 2019, KnowBe4 commissioned Forrester Consulting to evaluate security culture across global enterprises. The results were eye-opening. Forrester Consulting conducted an online survey with 1,161 respondents who all had managerial duties or higher

THE

A Problem of Definition

In that study with 1,161 respondents, there were 758 unique definitions given for security culture. Forrester analyzed these 758 unique definitions and broke them into five different categories based on the general sentiment reflected in each of the proposed definitions. Here's the breakdown:

- 29 percent of respondents believed that security culture is compliance with security policies.
- 24 percent said that it was having an awareness and an understanding of security issues.
- 22 percent said that it was a recognition that security is a shared responsibility across the organization.
- 14 percent indicated that it had something to do with establishing formal groups of people that could help influence security decisions.
- 12 percent said that a good security culture meant that security was embedded into the organization.

“

Security Culture:
The ideas, customs and social
behaviors of an organization
that influence its security.

”

“

**You get the culture
you ignore.**

John R. Childress

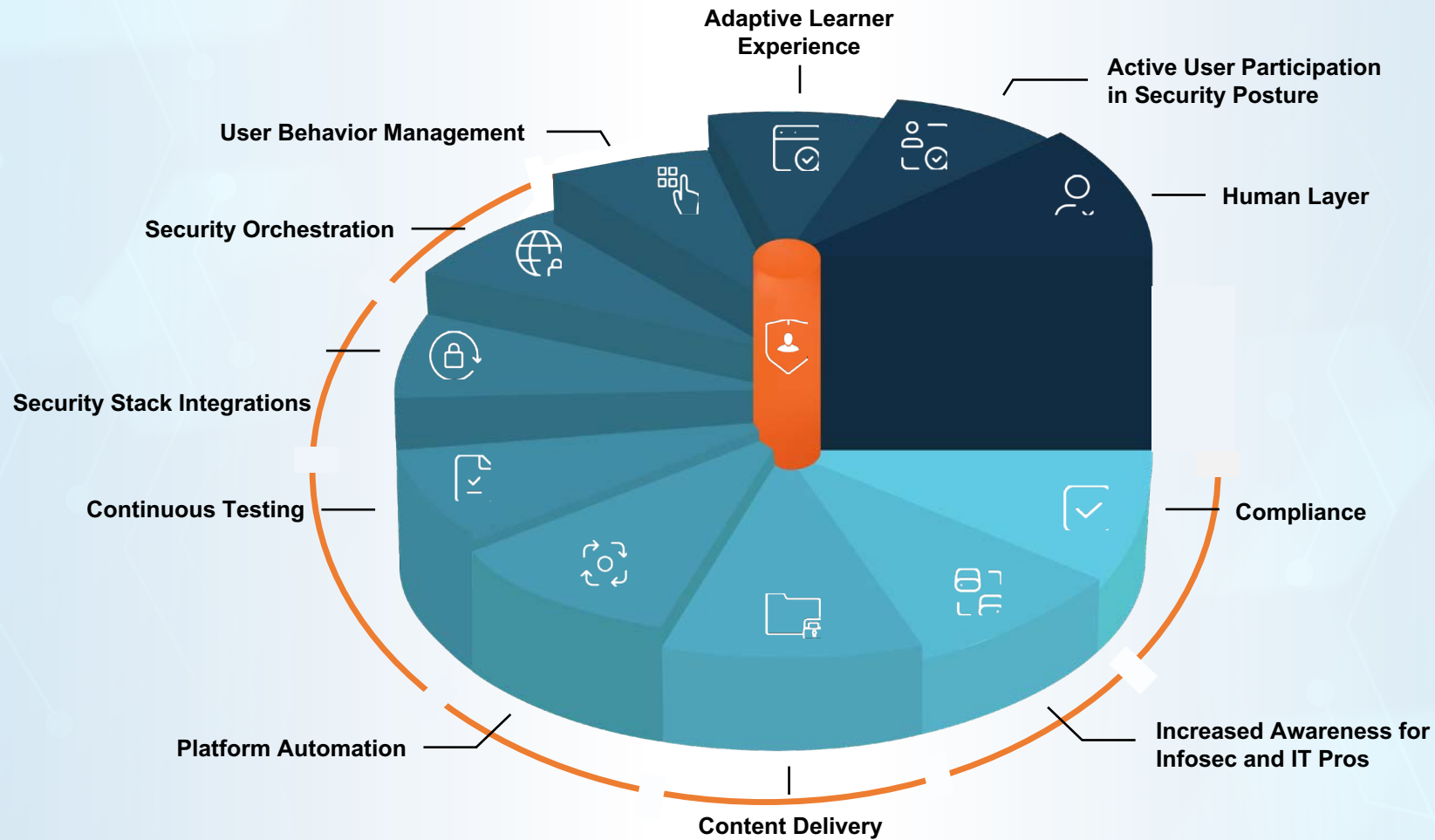
”

How Culture Relates to Awareness and Behavior



Industry Past, Present, and Future

FACILITATING THE ABCs: AWARENESS, BEHAVIOR, AND CULTURE



The Evolutionary Path of “Security Awareness”

In-House

The “Do-It-Yourself” era of in-house, ineffective offerings

Basic Content Vendors

Content and Newsletter vendors offering stale answers to a fresh problem

Phishing Simulation

The start of the first behavior management awareness programs

The rise of Ransomware created a market inflection point

Meaningful Metrics

Ability to report relevant analytics pertaining to behavior change, human risk, and engagement

Statistics interesting to executive teams, boards, regulators, auditors

Converges with the maturation of IT security as a discipline

Security Culture

The rise of security culture management

Awareness permeates throughout the entire organization

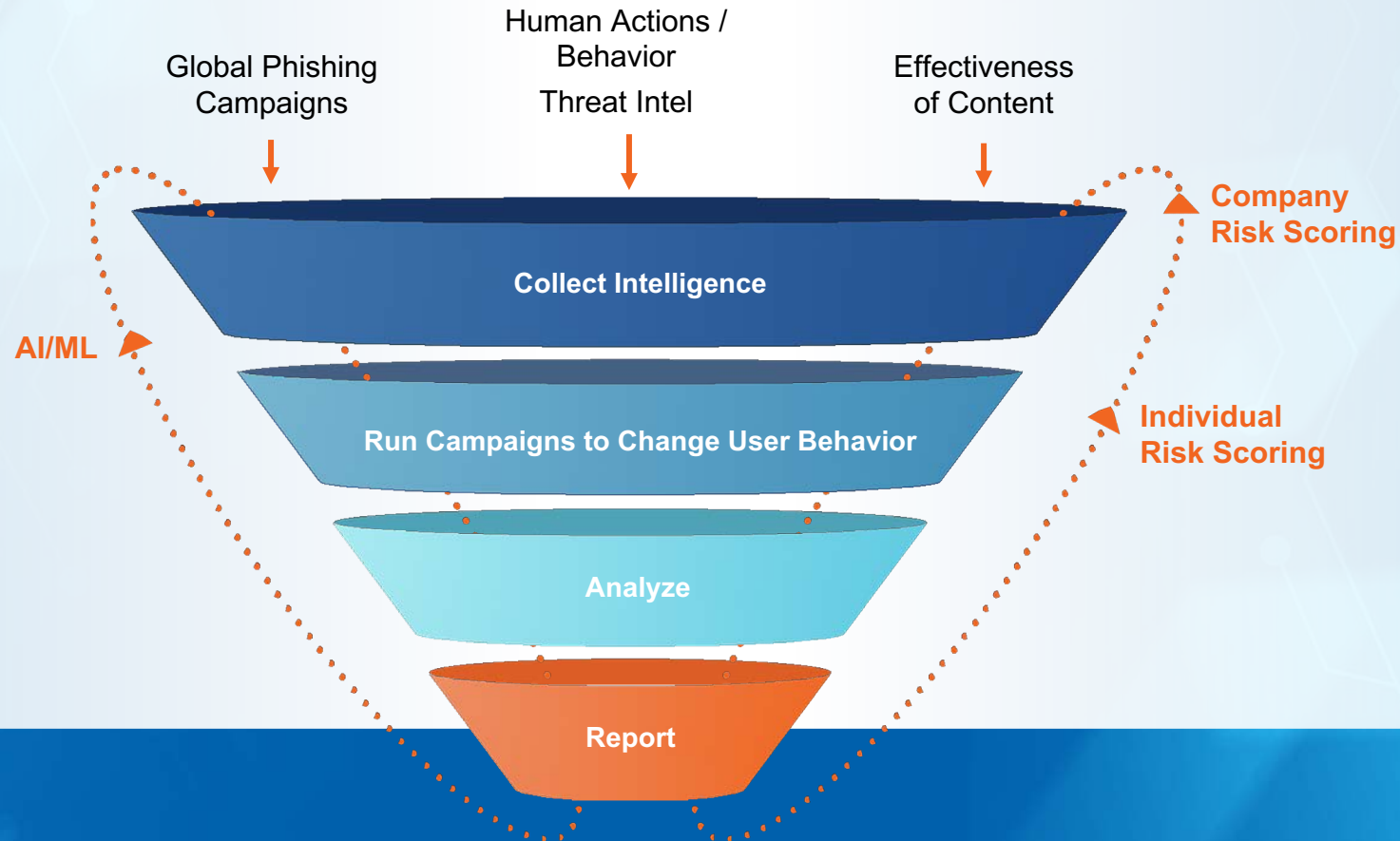
Collectively mitigates the risk of the human element

Converges with the maturation of the CISO role

A Data-Driven Advantage

Culture can be measured and modeled using several different elements. These range from training data elements, to simulated phishing resilience data, to organizational demographics, and more.

We call each of these datapoints, **Culture Maturity Indicators (CMIs)**.

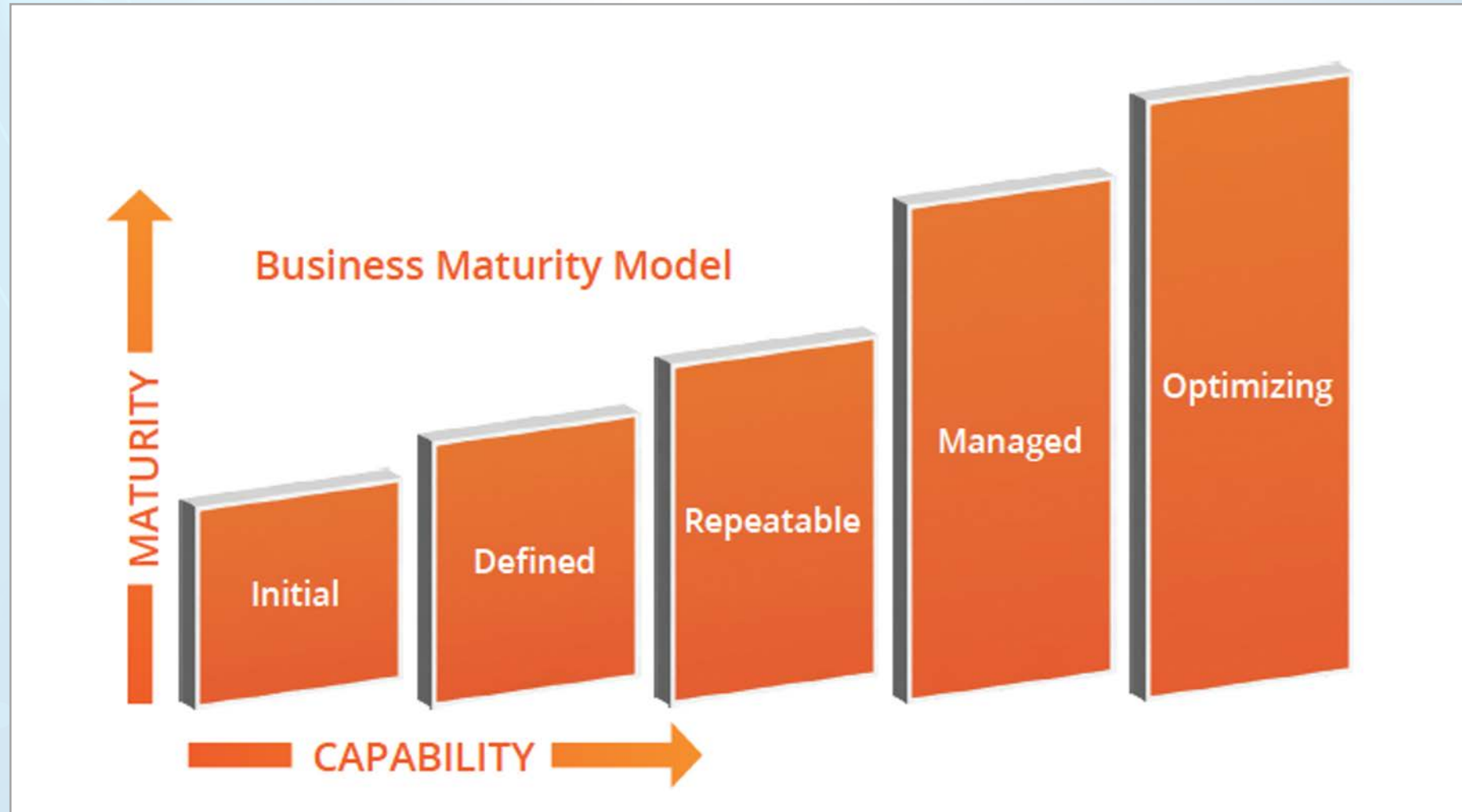


Example CMI

Security Awareness Training	Phishing & Simulated Phishing Testing	Behavioral Data Awareness	Organizational Tone and Activities	Survey Data	Other Measurement Data
<ul style="list-style-type: none"> • Frequency of training campaigns • Delivery types (in person, online, mobile, etc.) • Content types used • Learning modules taken • Measured areas of strength or weakness • Customization/ personalization for the organization and their unique risks • Customization/ personalization for the individual based on role/department 	<ul style="list-style-type: none"> • Opened • Clicked • Attachment open • Data entered on a landing page • Exploited: user clicked on an exploit enabled test • Macro enabled: macro on an attachment was enabled. • Replied • Reported • Accuracy of reporting • Organizational patterns of use for phishing simulations (e.g. customization of templates, gamification, etc.) 	<ul style="list-style-type: none"> • Tracking & Reporting of simulated or real-world user behavior alerts • Documented policies for user behavior failures (stick) or high performance in testing/ self-reporting (carrot) • Technology/ Integration into real-world behavior alerts • Gamification 	<ul style="list-style-type: none"> • Company-wide communications regarding security policies • Executive led discussion around security policies • Presence / absence of Security Champions Program • Reward and Contest regarding security behavior and culture including company-wide milestones, etc. • Security-centric special events 	<ul style="list-style-type: none"> • Culture Survey Data <ul style="list-style-type: none"> - Attitudes - Behavior - Cognition - Communication - Compliance - Norms - Responsibility • Proficiency Assessment Data <ul style="list-style-type: none"> - Password & Authentication - Email security - Internet use - Social media - Mobile devices - Security awareness • Others as desired 	<ul style="list-style-type: none"> • Phish-prone percentage • Industry Benchmarks • Virtual Risk Officer information • Email Exposure Check Data • API integration with other tools

Maturity models are helpful
... but most lack precision

Case in Point



Security Culture needs something better
...something more precise
... something data-driven

Seven Dimensions of Security Culture

Behavior

What I know

What I learn helps me to understand security. How I apply that knowledge affects security. I need to know *why* it matters for me to improve my behavior.

What I see

Do I see colleagues making an effort to be secure, or are my colleagues ignoring security measures because they "get in the way of business"?
How I behave is influenced by what I see around me.

What I hear

What I hear and what I see are not always the same thing.
Sometimes people do what they are told to by policy, and sometimes they make their own rules. Culture is shaped by our adherence.

What I say

How security and risk are being communicated in the workplace is a driver for secure behavior. *Are we talking about security? Is what I say positive or negative?*

What I feel

Emotions are a strong influence on our security behaviour. If employees feel like security is a nuisance, they are less likely to behave securely. Likewise, if they feel security is important, they are more likely to behave in a secure manner.

Responsibilities

Cognition

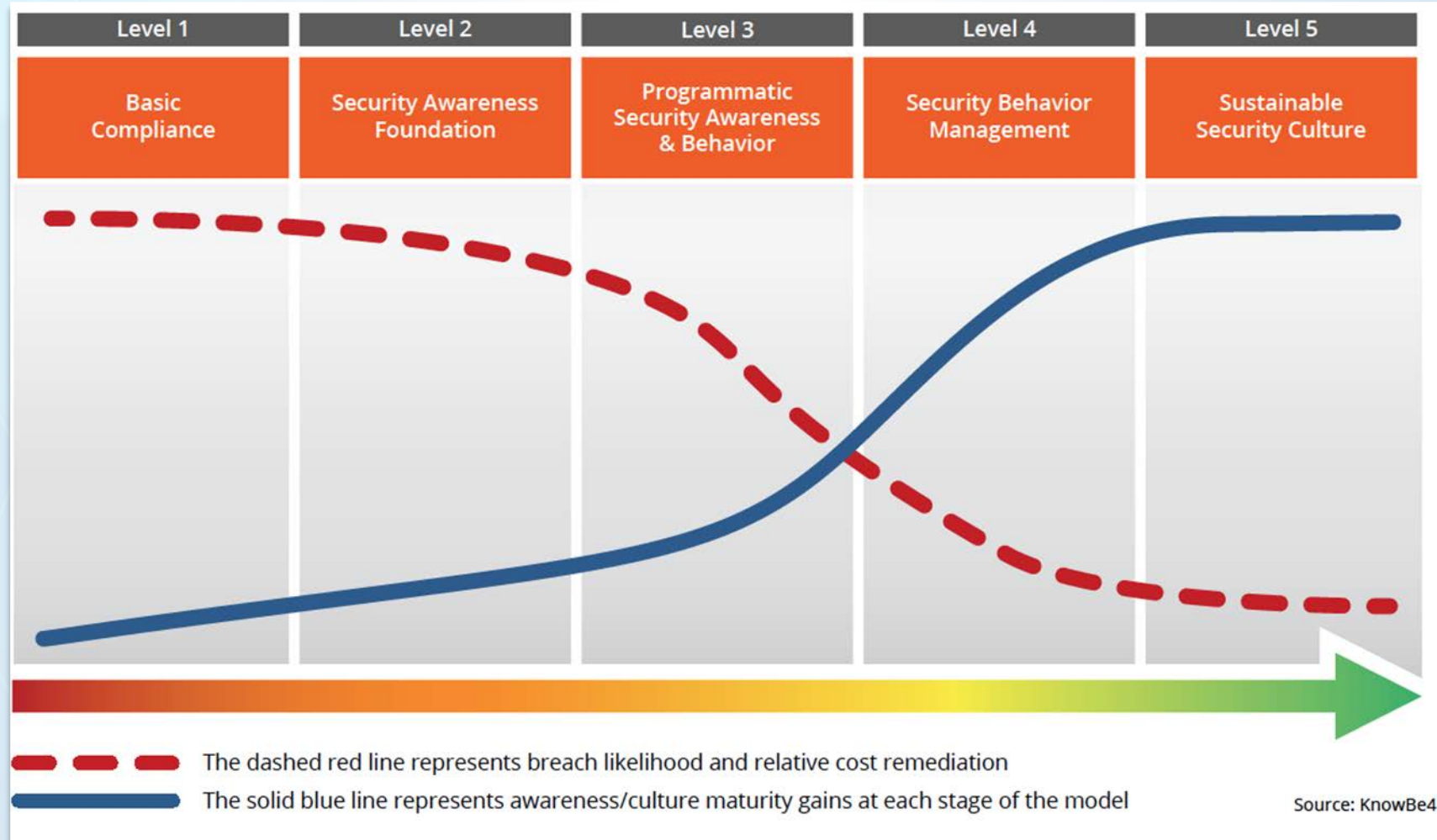
Norms

Compliance

Communication

Attitudes

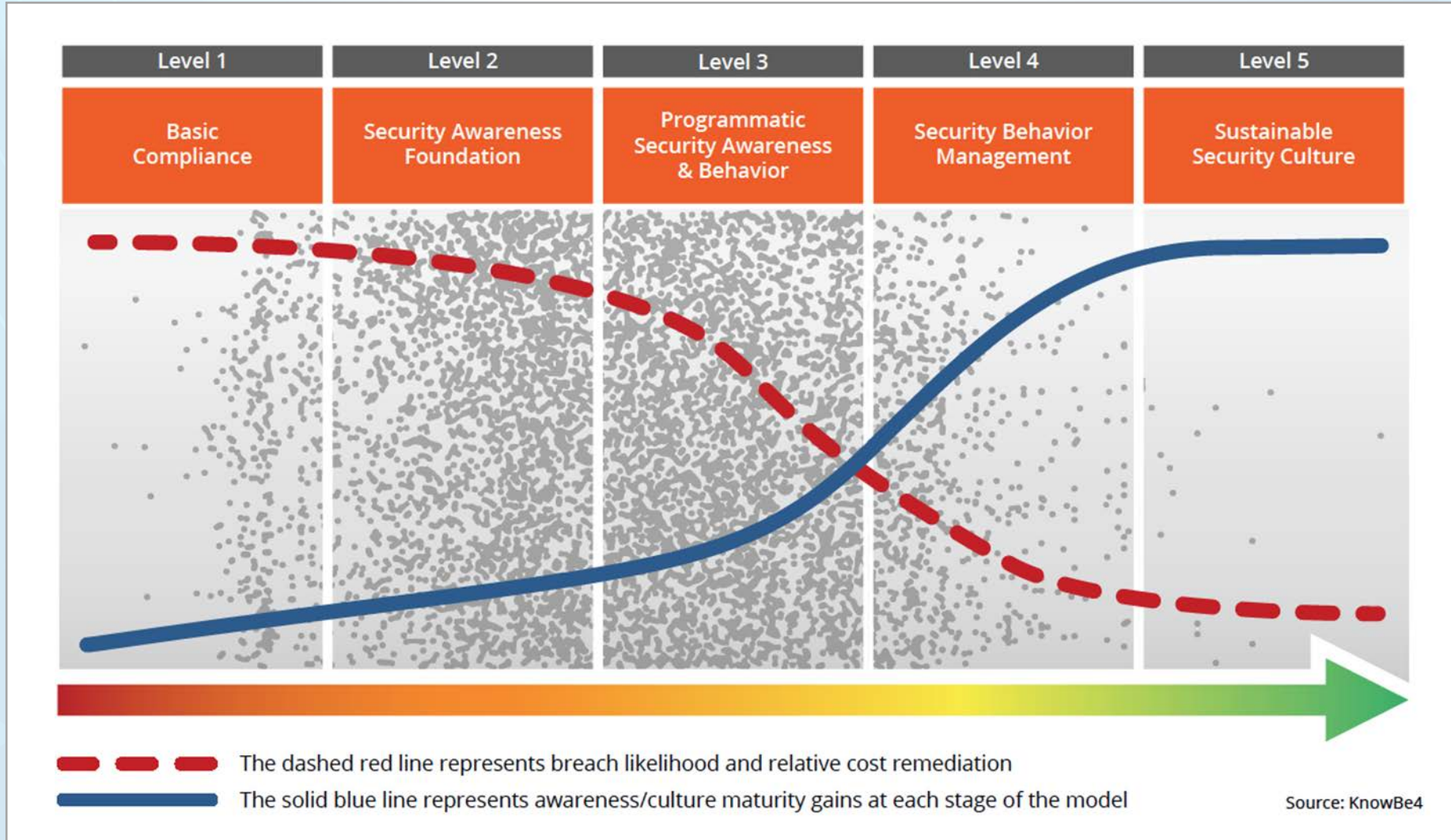
Introducing the Security Culture Maturity Model



One Model, Multiple Applications

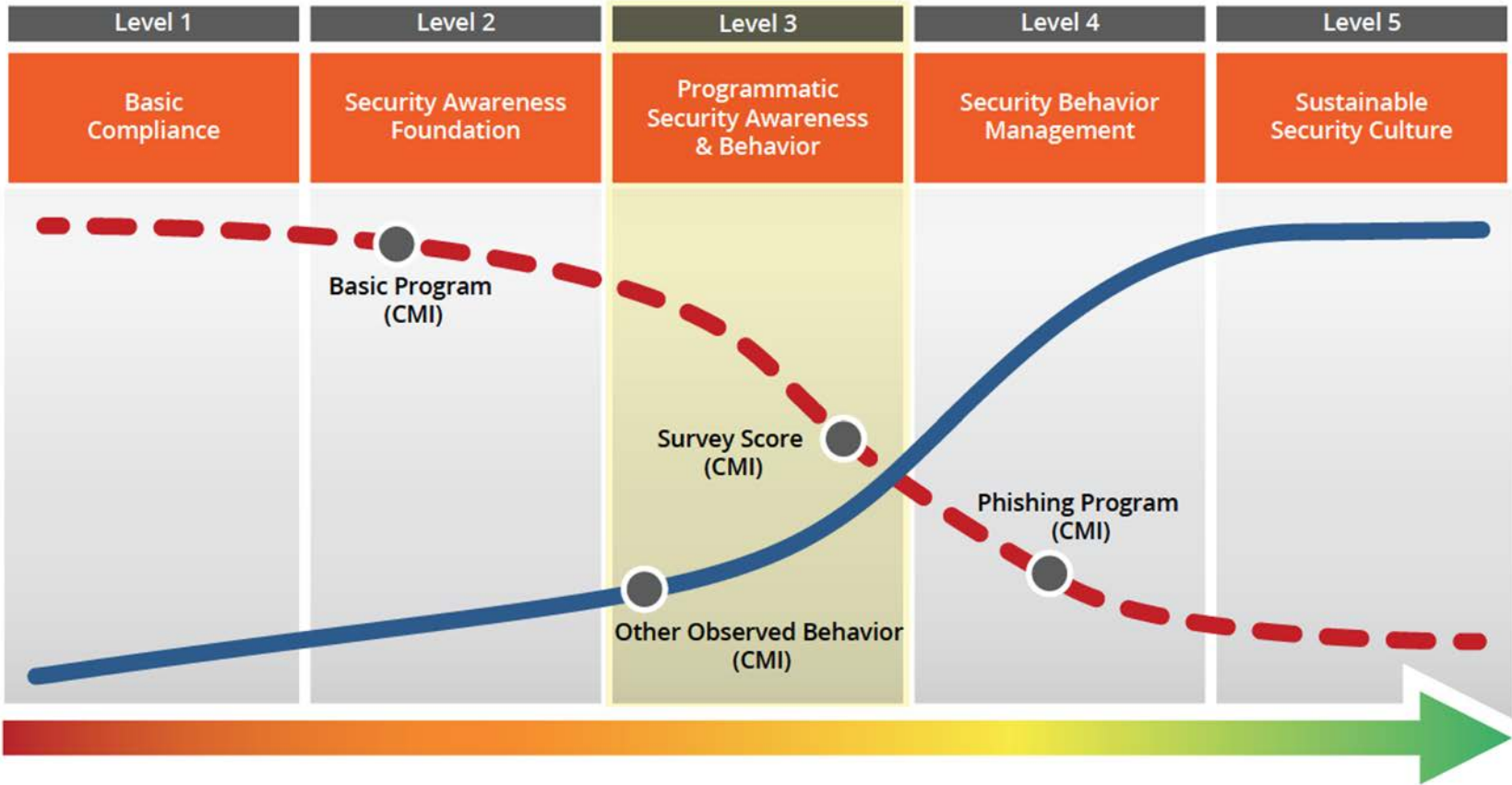


SCMM Example Data Overlay



SCMM Example Data Overlay

Current Maturity Given Available Data = Level 3

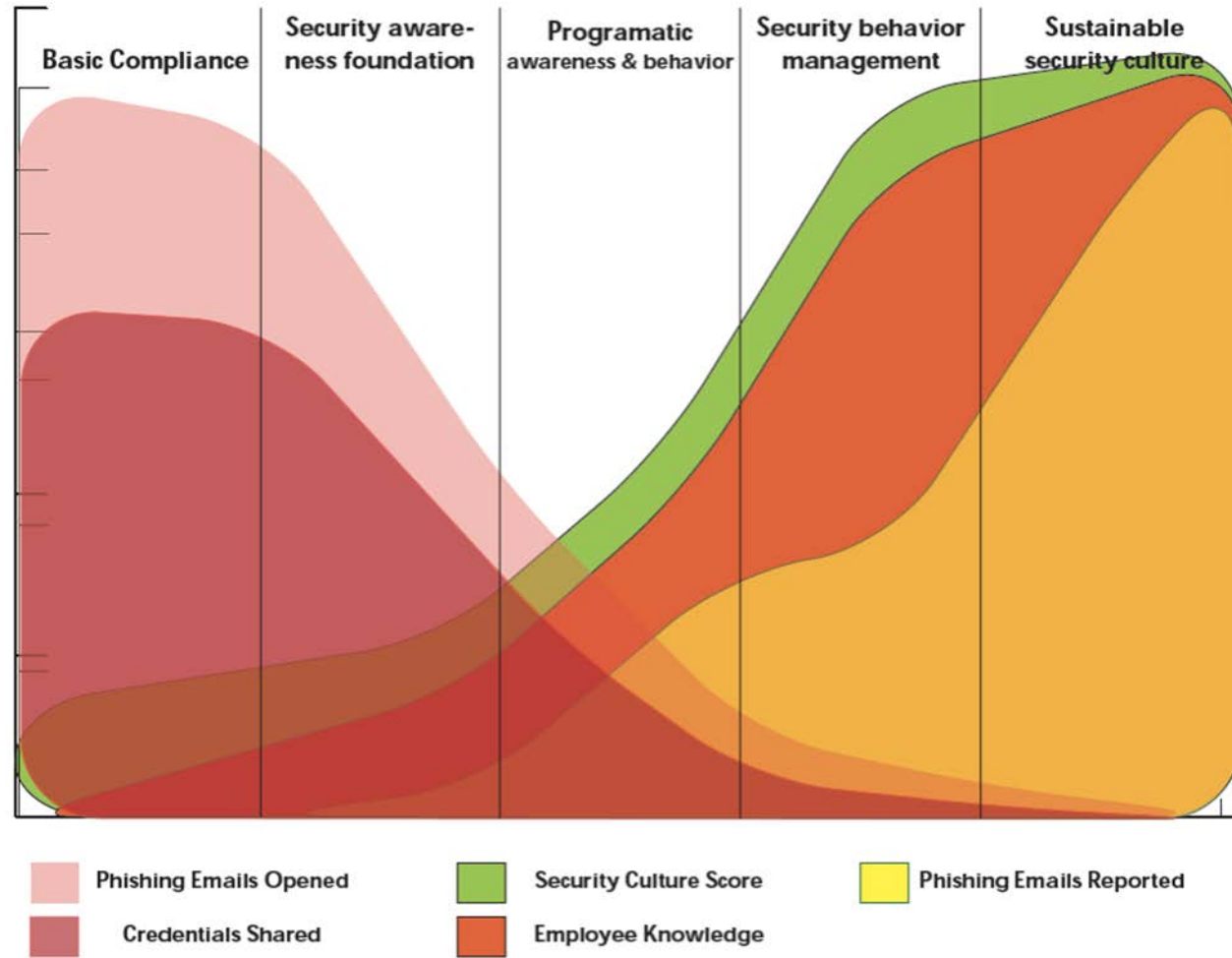


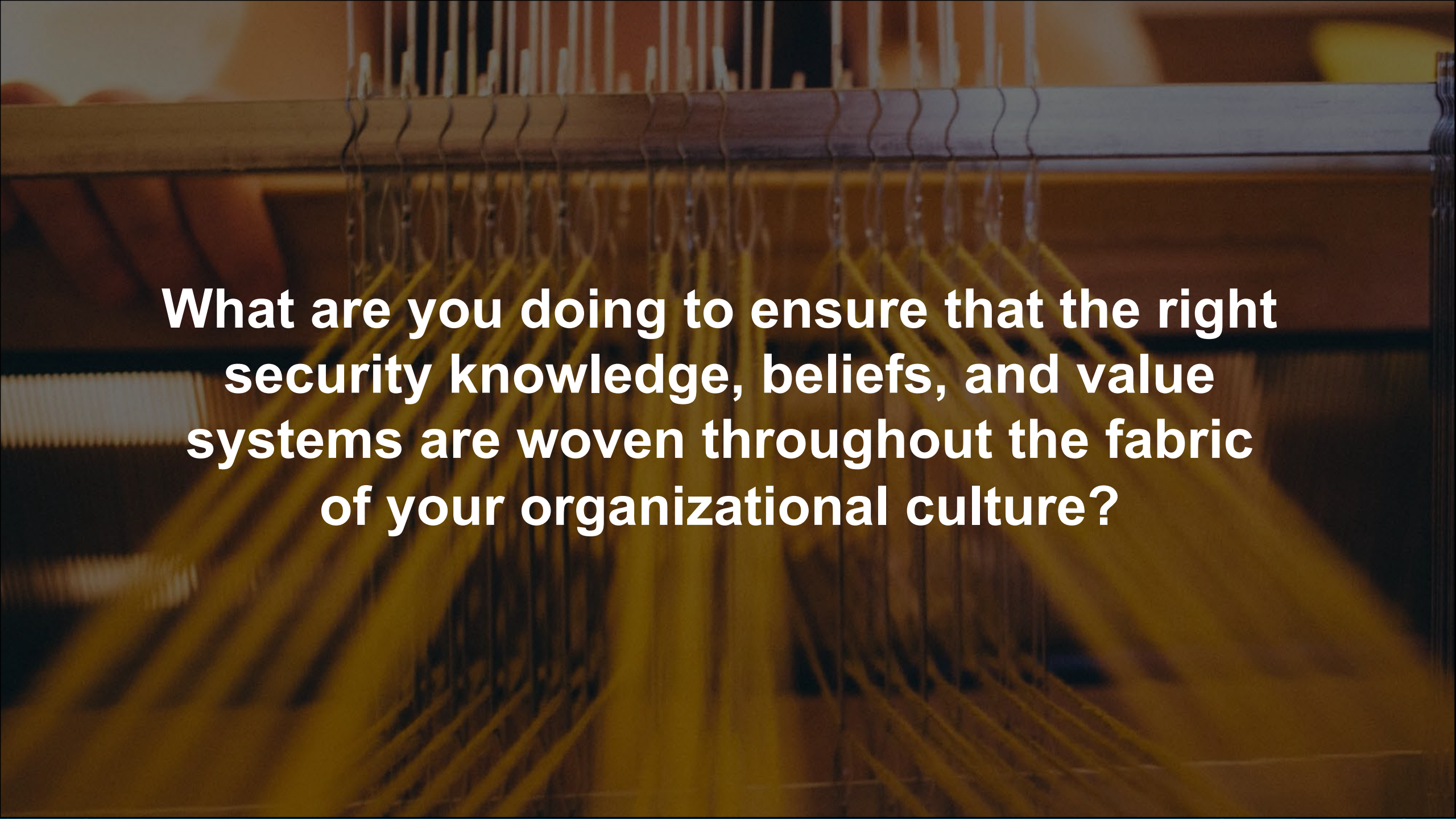
--- The dashed red line represents breach likelihood and relative cost remediation

— The solid blue line represents awareness/culture maturity gains at each stage of the model

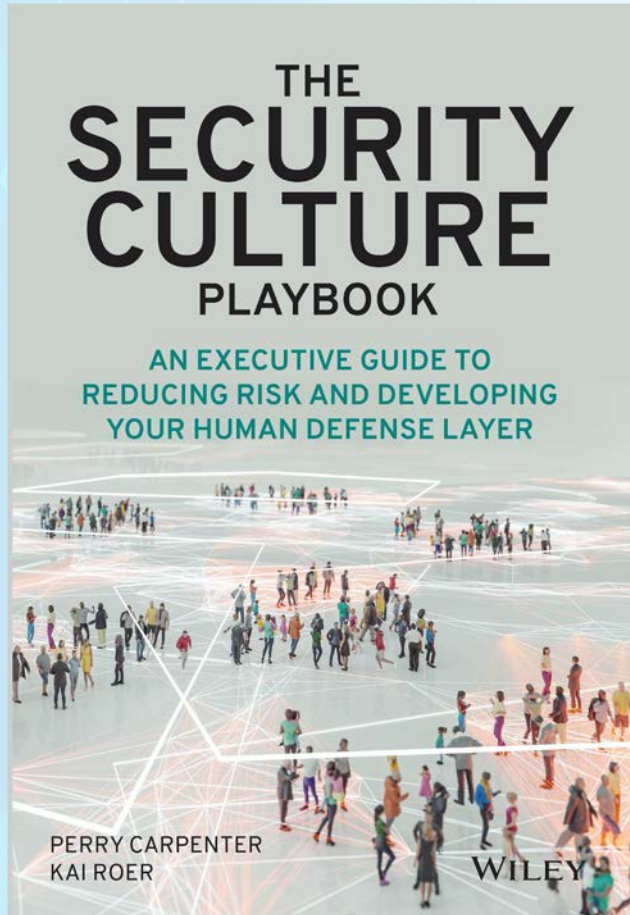
Source: KnowBe4

SCMM Example Data Overlay





What are you doing to ensure that the right security knowledge, beliefs, and value systems are woven throughout the fabric of your organizational culture?



The Security Culture Playbook

A concrete blueprint for producing real change, reducing risk, and proactively managing your company's exposure to cybersecurity threats. You'll also find:

- Revealing interviews from security culture thought leaders in a variety of industries.
- Strategies for bringing all the security culture pieces together into a coherent program.
- Actionable and modern insights from sociology and other academic disciplines.
- In-depth explanations of how to implement and shape behavioral outcomes, foster social pressures, and create positive patterns.