KnowBe4
Human error. Conquered.

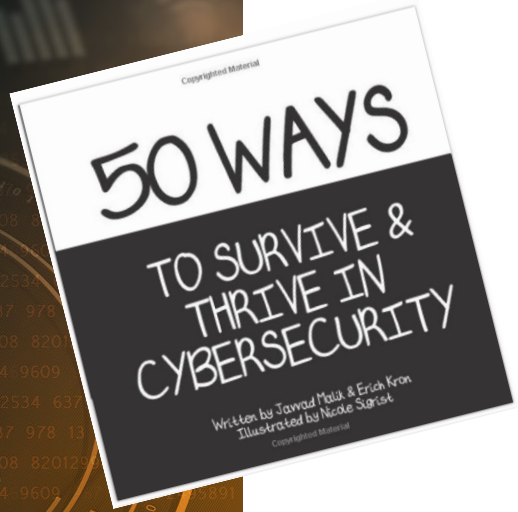
# Creating Culture:

## A Brief Look At Our Security Culture How-to Guide



Erich Kron
Security Awareness Advocate,
KnowBe4, Inc.

**Erich Kron**
**Security Awareness Advocate**




# About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, SACP, etc…
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for (ISC)$^2$
- A veteran of IT and Security since the mid 1990's in manufacturing, healthcare and DoD environments

CISSP® Certified Information Systems Security Professional

CISSP® Certified Information Systems Security Professional
ISSAP® Architecture

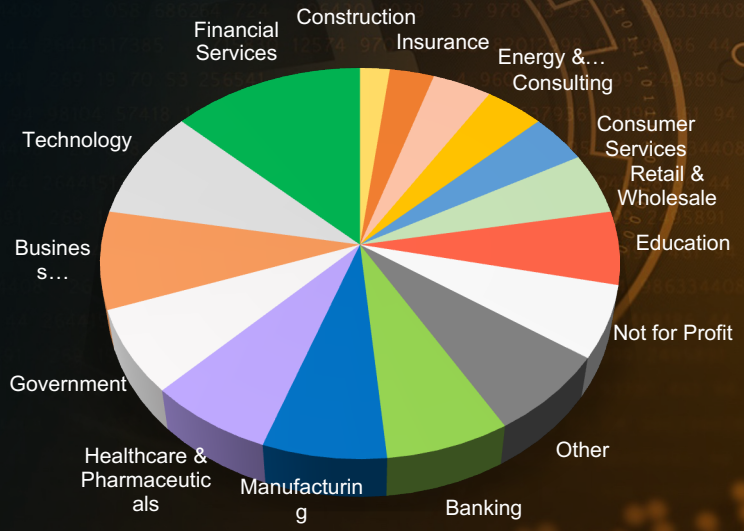
Microsoft® CERTIFIED IT Professional

KnowBe4
Human error. Conquered.

Over

# 60,000

## Customers




# About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

FORRESTER® WAVE LEADER 2022 Security Awareness And Training Solutions

Inc. 5000 AMERICA'S FASTEST-GROWING PRIVATE COMPANIES

Gartner peerinsights customers' choice 2021

# Agenda

- What is culture?
- A culture focused program
- Building culture

# Agenda

- What is culture?
- A culture focused program
- Building culture

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?

# Defining “Culture”

**Organizational culture** is not the sum of roles, processes and measurements; it is the sum of subconscious human behaviors that people repeat based on prior successes and collectively held beliefs.

**Similarly**:

**Security culture** is not (just) related to "awareness" and "training"; it is the sum of subconscious human behaviors that people repeat based on prior experiences and collectively held beliefs.

# Culture is:

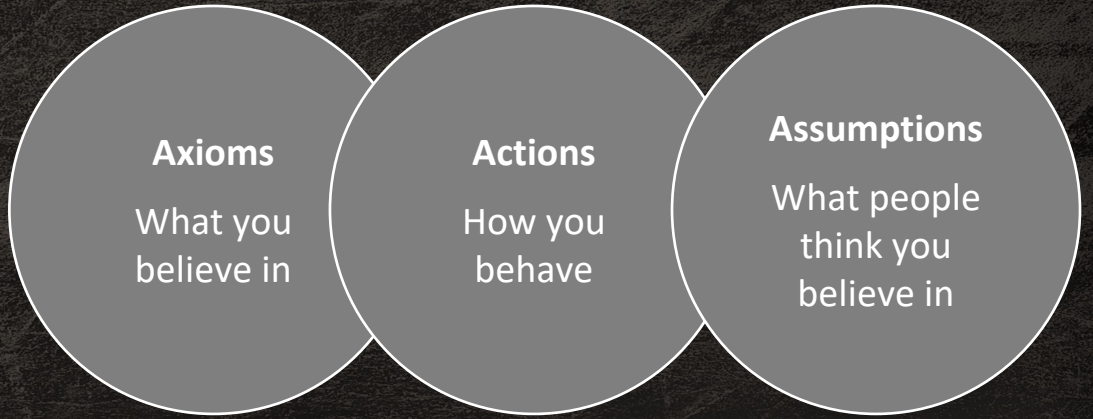
- Shared
- Learned
- Adaptive
- Integrative
- Prescriptive:
  - Rules
  - Patterns
  - Assumptions
  - Beliefs

# Leaders Are Cultural Beacons: Are They Sending the Right Signals?

## Leaders lead:

- Explicitly
- Implicitly
- Symbolically
- Representationally
- Constantly

### Three dimensions of trust and integrity



# Agenda

- What is culture?
- A culture focused program
- Building culture

# Secrets to a Higher Impact Program

1. Take stock of where you are and where you are going
2. View awareness through the lens of organizational culture
3. Leverage behavior management principles to help shape good security hygiene
4. Be realistic about what is achievable in the short-term, and optimistic about the long-term payoff

# Secret 1

Take stock of where you are and where you are going

# Secret 1: Look at your surroundings!

Take stock of where you are and where you are going

- Interview different divisions, leaders, and employees at all levels to get a sense of where everyone currently is
- Outline your goals for the year

# Consider how/where awareness fits within each element of the Cyber Security Framework

# Secret 2

View awareness through the lens of organizational culture

**Traditional awareness efforts are based on the belief (or hope) that information leads to action.**

---

In other words …

the problem with awareness is that "awareness" itself does not automatically result in secure behavior.

# The traditional security awareness formula suffers from a fundamental logic error

**Traditional security awareness seems to be based on this formula:**

*Person* + *Information* =

*Desired Actions* and *Beliefs*

***P*** + ***I*** = ***DAB***

# Secret 3

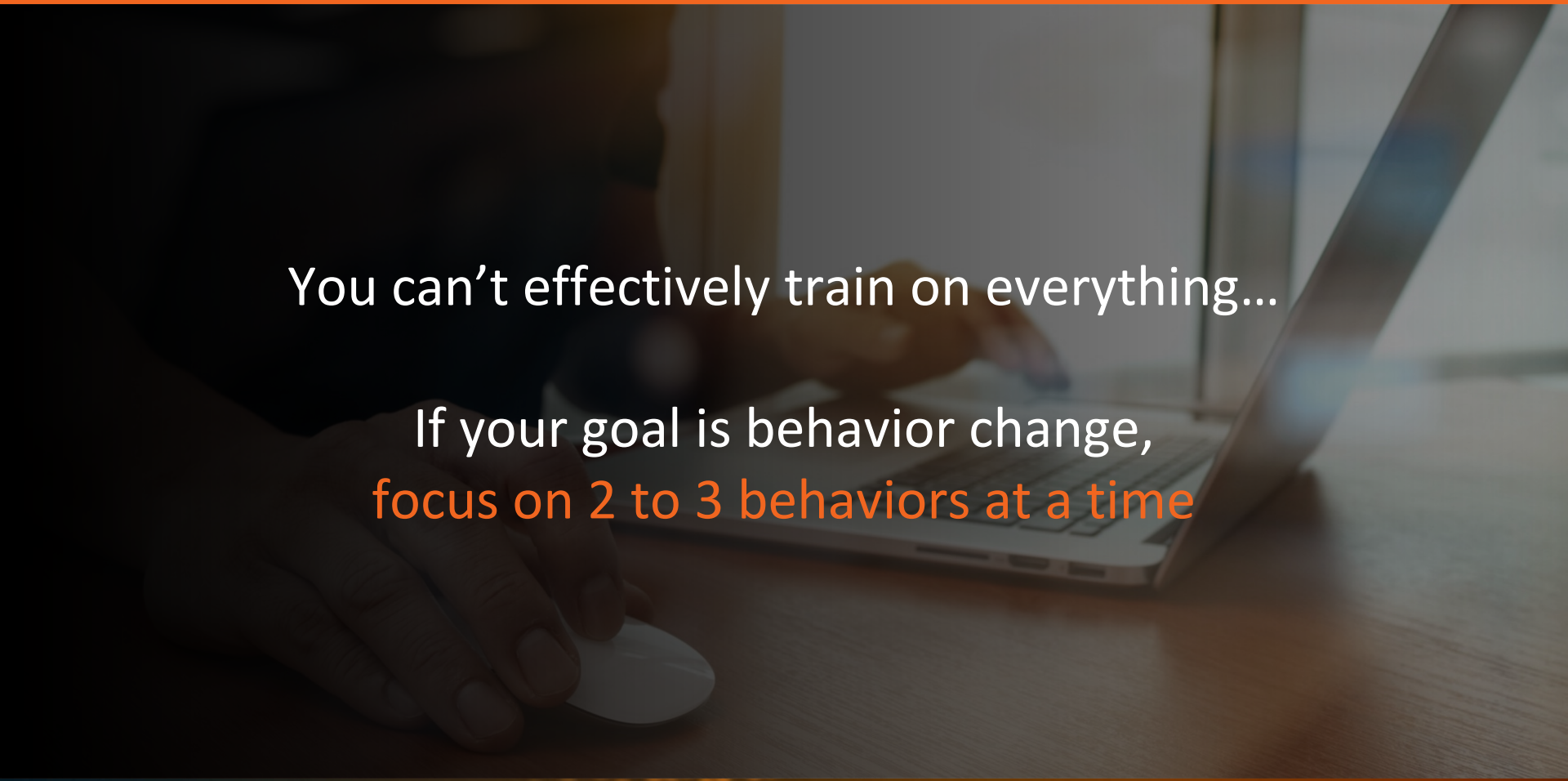
Leverage behavior management principles to help shape good security hygiene

# *Security Awareness* and *Secure Behavior* are NOT the Same Thing

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

***Ask yourself:***

*Do you care more about what your people* ***know*** *or what they* ***do****?*



You can’t effectively train on everything…

If your goal is behavior change,
focus on 2 to 3 behaviors at a time

# *Nudge* them in the right direction

A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not.

**Nudge**: Improving Decisions About Health, Wealth, and Happiness, 2008


http://www.abc.net.au/radionational/programs/allinthemind/better-life-decisions-with-behavioural-economics/6798918

By WissensDürster at German Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=31542169

# Secret 4

Be realistic about what is achievable in the short-term, and optimistic about the long-term payoff

# Be a realistic optimist!

## Consistency is key…

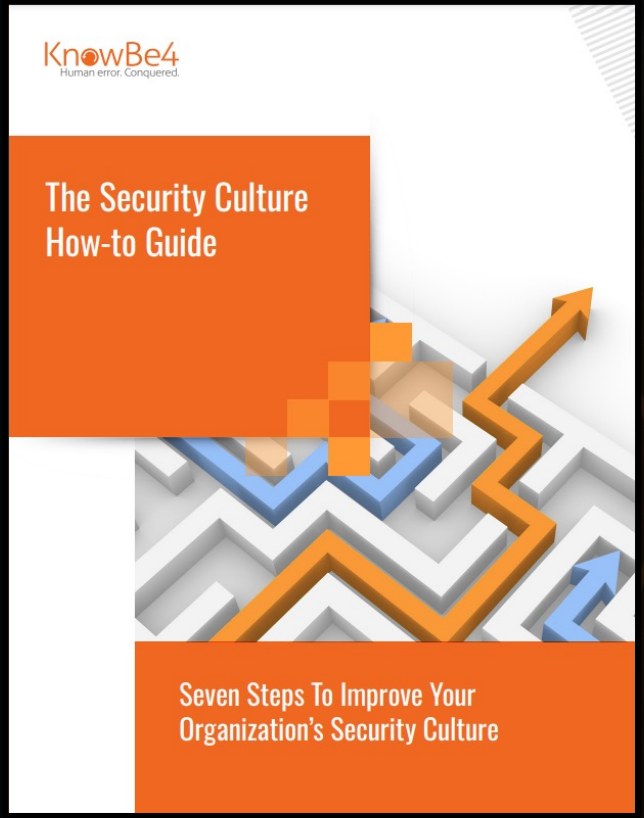
## …commit to persevere

# Know Your Place and Scope of Influence!

Culture is led from the **very** top of the organization; it doesn't originate from you or your group.

# Agenda

- What is culture?
- A culture focused program
- Building culture




# A helping hand when building culture

Security culture is becoming a popular topic in the industry, however many people don't understand what it means, or how to get to building a good, strong culture. There are many questions about this, so we came up with 'The Security Culture How-to Guide' to help you get started.

In this guide we identified 7 steps that will help people better understand the process of improving their security culture.


https://info.knowbe4.com/cltre-seven-dimensions-security-culture

In the 2019 research paper we published called “The Seven Dimensions of Security Culture,” the authors identify seven dimensions of security culture and explain how they are used to measure an organization’s security culture.

The seven dimensions are:

- Employee attitudes to security and policies
- Behaviors
- Cognitive processes surrounding security
- Quality of communication
- Compliance to security policies
- Organizational unwritten rules or norms
- Individual responsibilities

We will not be going into detail on these dimensions; however, they may be mentioned.

# The 7 steps:

The 7 steps we identified for creating a security culture are as follows:

- Step 1 – Choose One or Two Behaviors You Would Like to Change
- Step 2 – Design a Plan to Influence Behaviors on an Organizational Scale
- Step 3 – Get Leadership Buy-in
- Step 4 – Communicate
- Step 5 – Execute the Plan
- Step 6 – Measure Results
- Step 7 – Determine the Move Forward Strategy

# Step 1:

## Choose One or Two Behaviors You Would Like to Change

An issue that often plagues people when tying to deploy security awareness programs, or improve culture, is to attempt to accomplish too much at one time. While it's great to want to make big changes quickly, if you focus on everything, you are not actually focused on anything.

- The behaviors they choose to address should align with the top organizational risk.
- A Security Culture Survey may help identify which behaviors to focus on
- Give ample time for the change
- Once they have run through a cycle or two, you may be able to adjust the cadence

# Step 2:

## Design a Plan to Influence Behaviors on an Organizational Scale

Behaviors can be directly influenced through formal means, like in the case of a policy creation or change, or can be done informally and socially, especially through demonstration by leadership. For example, a leader that locks their computer every time they walk away from it, demonstrates how important is to others, even if they don't realize it.

- Identify people who can help influence these changes, even if they are not in your own department and use them as champions
- Treat this like a planned technology rollout, accounting for dependencies and risk mitigation

# Step 3:
## Get Leadership Buy-In

Prepare an executive summary for leadership that is light on the details but heavy on **why** the changes need to happen, the risk to the organization if the changes do not occur, who will be involved in the plan, the resources you will need, and the intended timeline.

- If possible, get a commitment from leadership to adopt and display the desired behavior changes to the rest of the organization.
- do not ask for an unreasonable commitment on the executive's behalf

# Step 4:
## Communicate

Step Four is all about communicating the “why” to the people whose behavior we are looking to change. This is more important than it may initially seem because we are often asking people to take additional steps to accomplish the same thing they have in the past.

- Illustrate how the behavior change is personally relevant to them as employees
- This is great place to engage with your identified champions within the org to help communicate at a peer level
- work with other departments across the organization to reinforce the messaging in their respective communications

# Step 5:
## Execute the Plan

Your plan should have a clear goal with a well-defined picture of what success looks like. Deadlines and the times to communicate and implement each part of the plan should already be thought out. Some flexibility in the plan is to be expected, but keep an eye on the goal and measure progress, when possible, along the way.

- It's a great time to perform a Security Culture Survey so you have a baseline to compare improvements to
- Be ready to experience some push back against changes, but don't take it personally
- Keep an eye open for things that negatively impact the workforce and be ready to adjust if needed

# Step 6:
## Measure Results

When the plan is fully executed, performing another Security Culture Survey will illustrate where you have made progress and areas where more progress might be needed. Use this information to find the approaches that work within your specific organization so you can implement them in future cycles

- Remember to document the results in a report that can be shared with leadership
- Note where the behavior changes in one dimension impact others so you can better understand the relationships for future planning

# Step 7:

## Determine the Move Forward Strategy

Once you have met the timeline allotted for the plan or have met the goals outlined in the plan, you can review your threats and determine if you should continue to focus on the same goals or work toward others in the next cycle.

- Review what worked well and what did not
- Reach out to the people you identified as advocates and get their feedback and suggestions
- Continue reinforcing the behaviors you have been working on, even if you move to a new behavior focus

# Summary:

Improving security culture may seem complex, however, understanding that change happens over time and is the result of positive behavior changes and habit formation, can simplify the task.

Be deliberate in your actions and do not try to change too much too quickly.

Communication can make a big difference in the swiftness and degree to which the behaviors change, especially if the communications help people understand why they should care about security.

# Thank You!


## Erich Kron – Security Awareness Advocate

ErichK@KnowBe4.com | @ErichKron


KnowBe4
Human error. Conquered.


Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com