NSSF®

The Firearm Industry Trade Association

PROJECT CYBERSAFE™

Security is Everyone's Business

Presented by:

Joanna Huisman

SVP Strategic Insights & Research at KnowBe4

Additional NSSF Compliance Resources

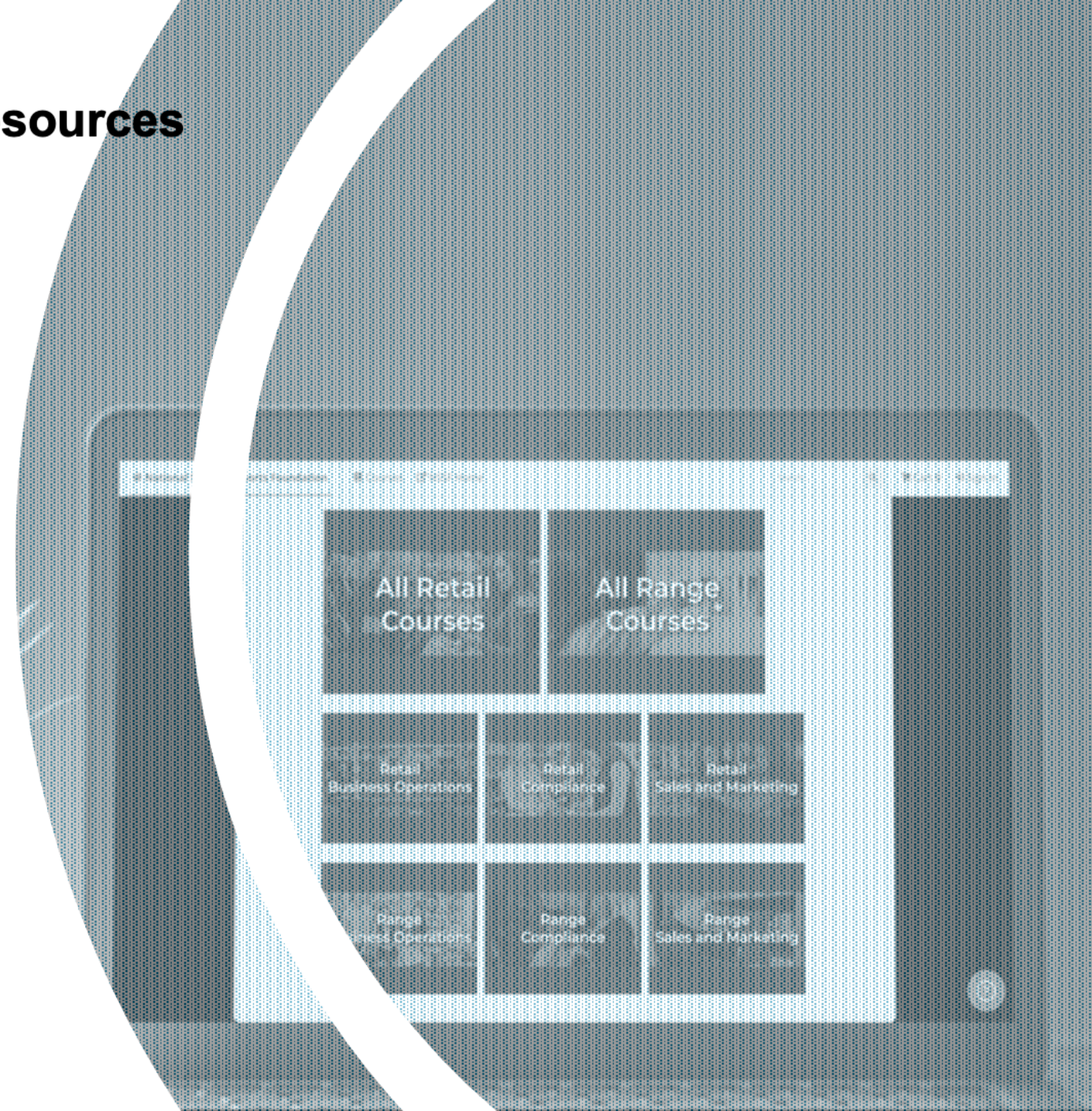
NSSF
The Firearm Industry Trade Association

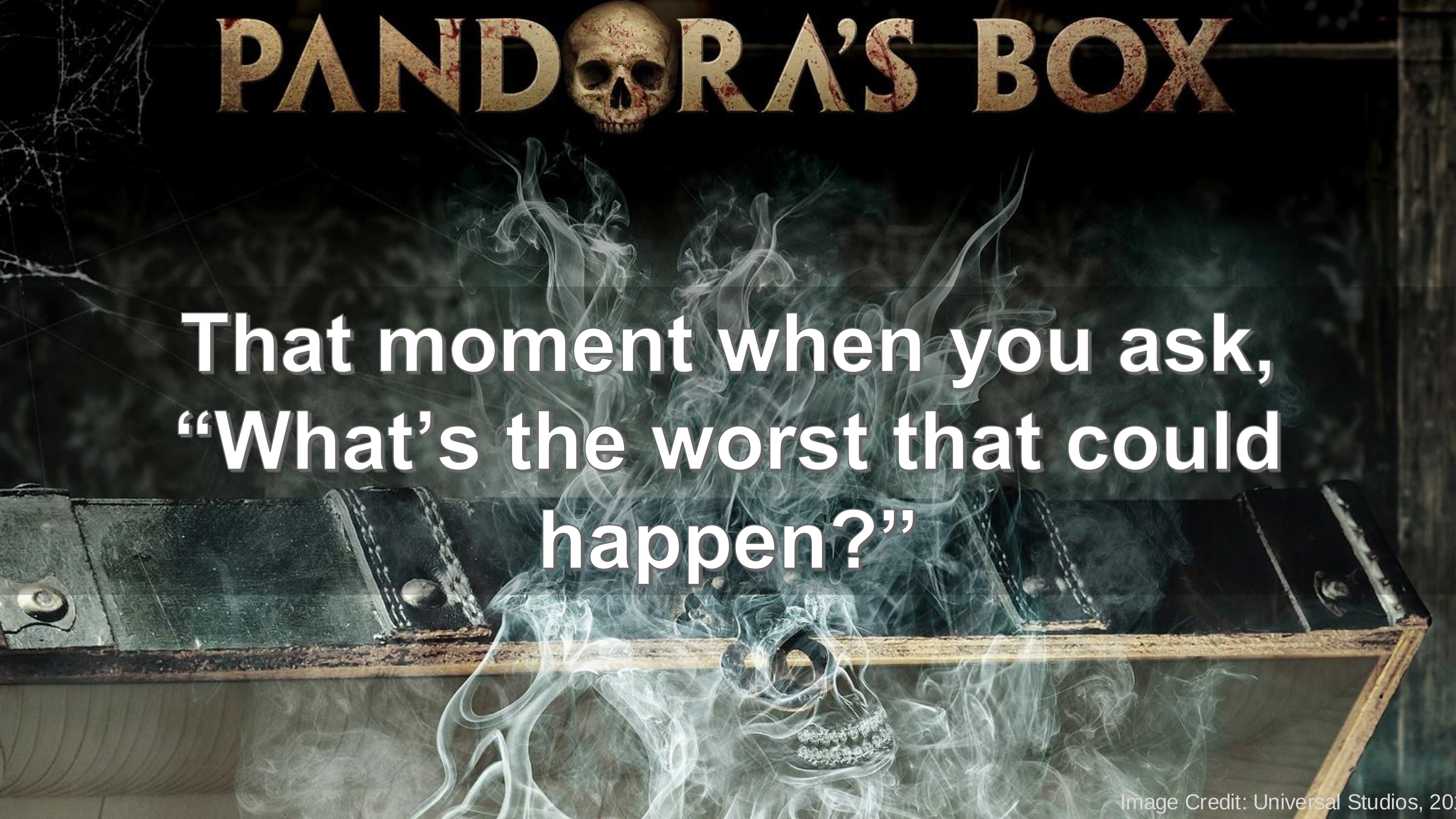
SHOT UNIVERSITY™
NSSF® online

Industry Compliance courses:

- “Zero Tolerance” Policy
- Winning at ATF Inspections
- Completing the Form 4473
- Multiple Sales Report
- and more

NSSF.org/Education


All Retail Courses
All Range Courses
Retail Business Operations
Retail Compliance
Retail Sales and Marketing
Range Business Operations
Range Compliance
Range Sales and Marketing



That moment when you ask, "What's the worst that could happen?"

Image Credit: Universal Studios, 20

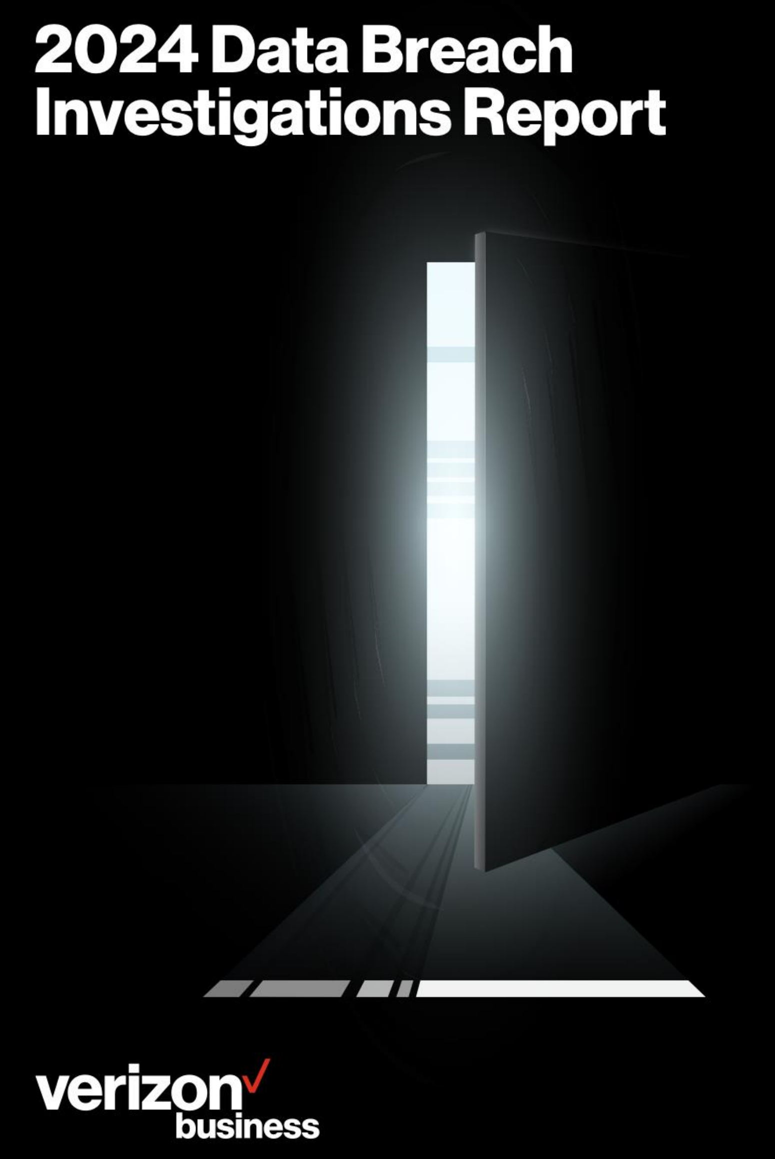
If you discovered burglaries were occurring in your neighborhood, what would you do to protect your home?

!
Warning
The system may have found viruses
Do you want to stay signed in?
Yes,Keep me signed in
No,Sign me out

If you discovered cybercriminals were stealing data from other organizations, what would you do to protect your organization?

Agenda

1. The Threat Landscape
2. Phishing benchmark data by industry
3. Your Security Culture & “Human Firewall”



2024 Data Breach Investigations Report

verizon business

According to Verizon’s 2024 Data Breach Investigations Report, human error was often a contributing factor to data breaches, playing a role in 68% of cases occurring through accidental actions, the use of stolen credentials, social engineering and even through malicious privilege misuse.

However, the report authors excluded privilege misuse from the calculation of the human element to better assess the impact of security awareness programs. Notably, the findings indicate that the human element continues to play a significant role, indicating that mitigating human-based risk should be a key priority for organizations.

The Threat Landscape is

All of Us

All the Time

Everywhere

In All Contexts of Life

Lazy…

Distracted…

Lacking the knowledge.

How The Bad Guys Attack

This email icon is totally
free. For noncommercial use!
If you like this icon use :)

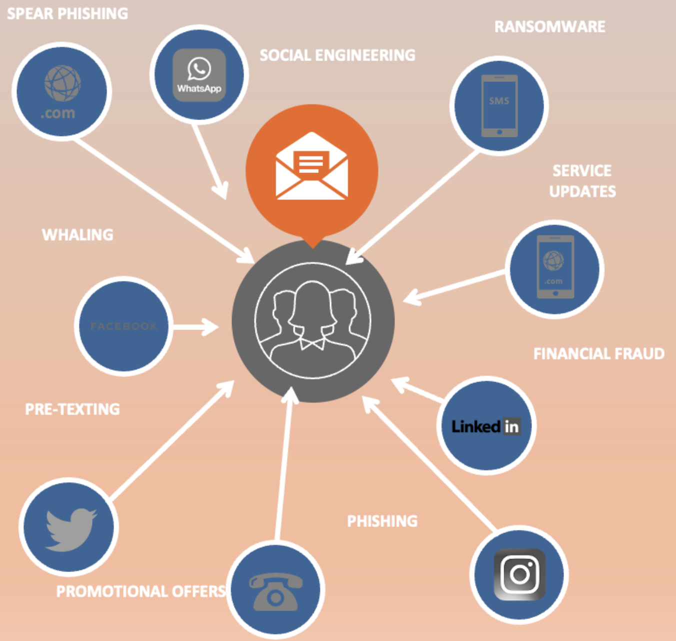
A cybercriminal does a 'deep search' for email addresses of your organization on the Internet

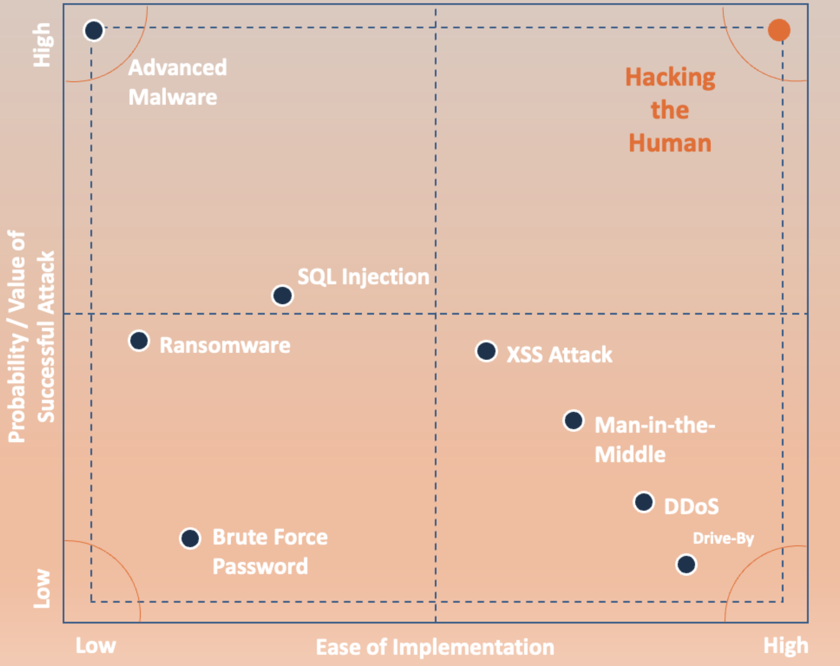
They find all publicly available email addresses of your employees

They use these to launch a phishing attack on as many employees as possible

It works and it's easy

Social Engineering is Popular Because it Works!



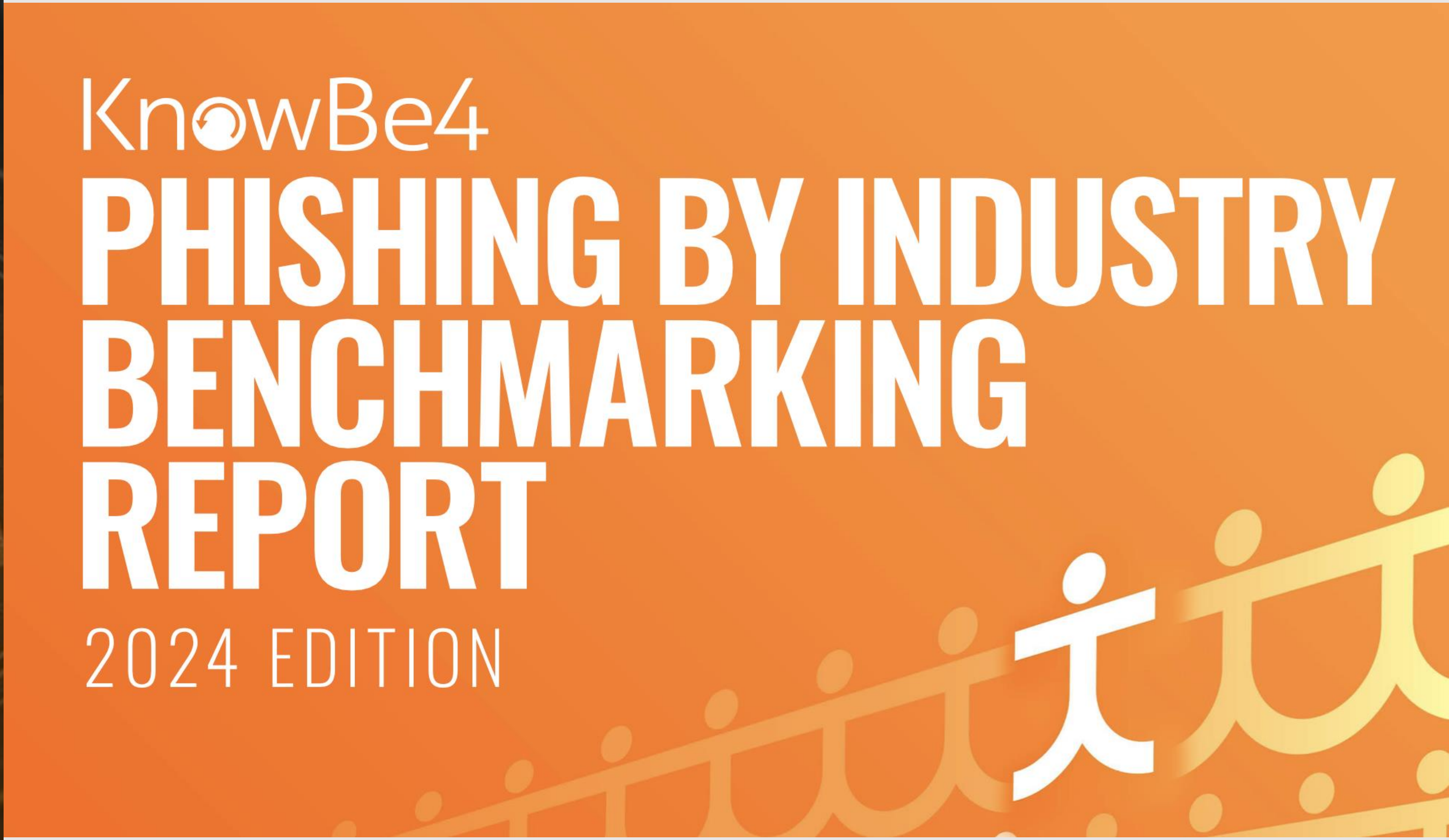


KnowBe4
Human error. Conquered.

Agenda

1. The Threat Landscape
2. Phishing benchmark data by industry
3. Your Security Culture & “Human Firewall”

The question every executive asks...



KnowBe4

PHISHING BY INDUSTRY BENCHMARKING REPORT

2024 EDITION

METHODOLOGY AND DATA SET

54.1M
Phishing Security Tests

11.9M
Users

[illegible]7K
Organizations

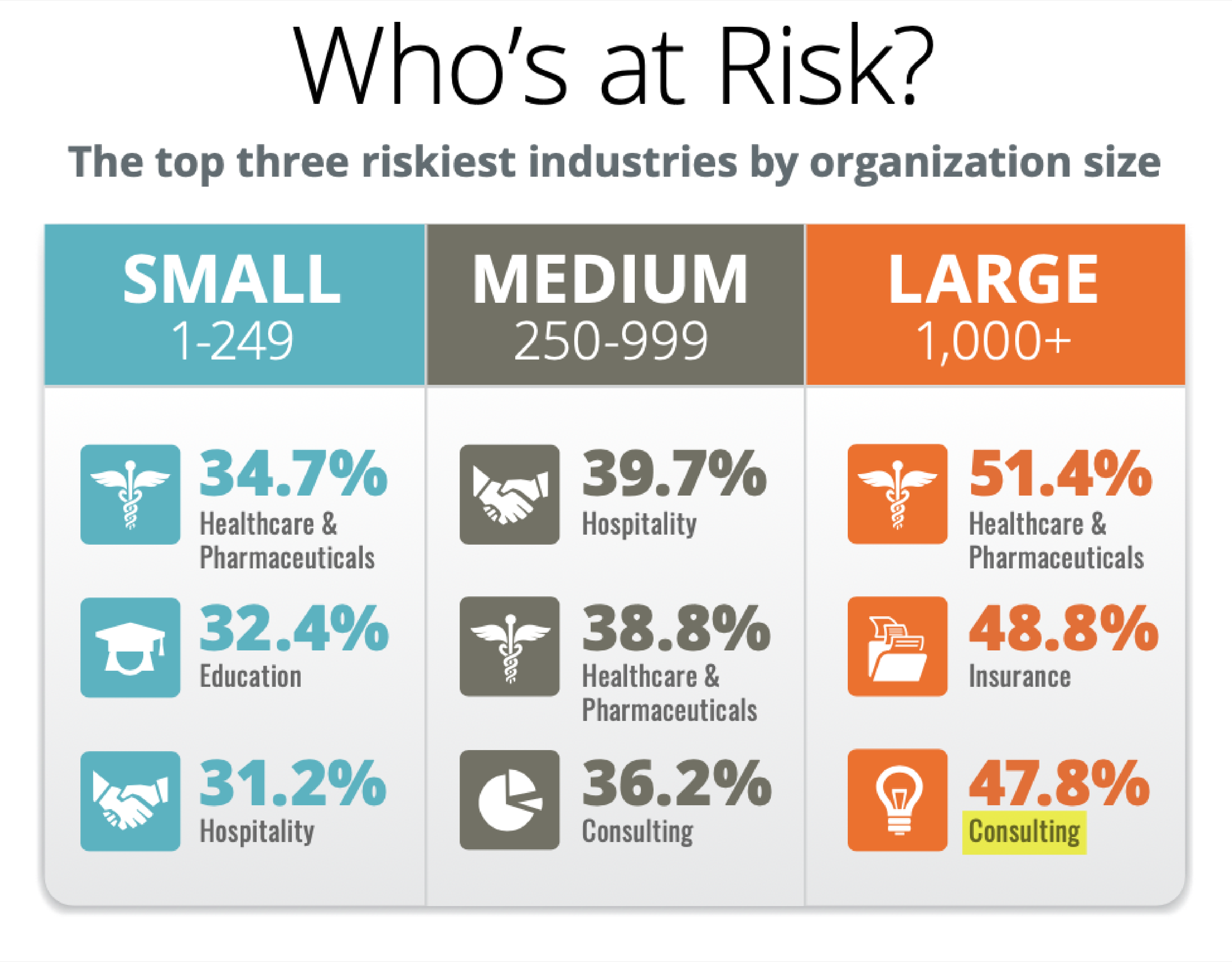
19 INDUSTRIES

- Banking
- Business Services
- Construction
- Consulting
- Consumer Services
- Education
- Energy & Utilities
- Financial Services
- Government
- Healthcare & Pharmaceuticals
- Hospitality
- Insurance
- Legal
- Manufacturing
- Not For Profit
- Other
- Retail & Wholesale
- Technology
- Transportation

ORGANIZATION SIZE RANGES

42,488 Organizations	9,934 Organizations	3,253 Organizations
1-249	250-999	1000+

RISKY BUSINESS



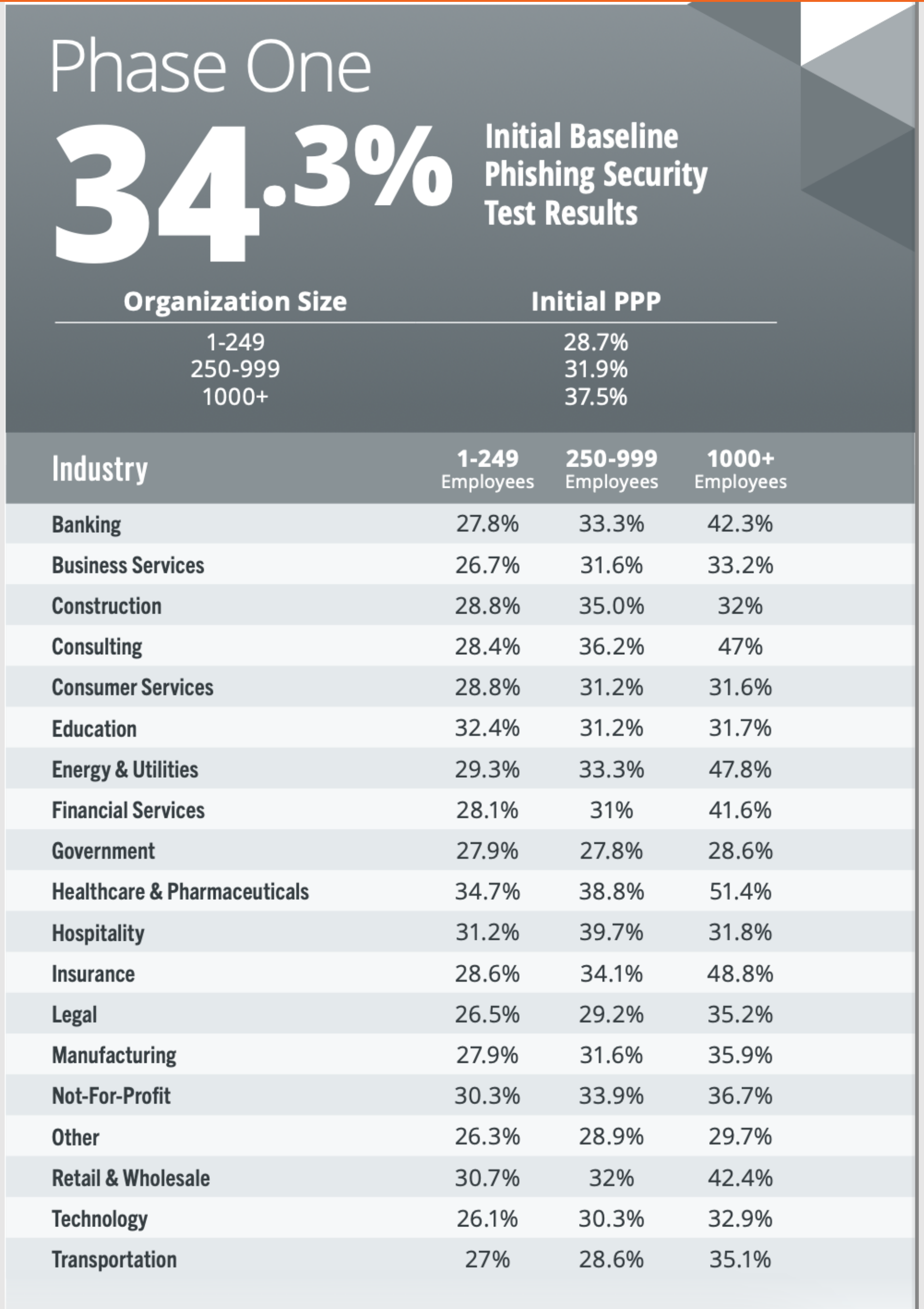
Who’s at Risk?

The top three riskiest industries by organization size

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
34.7% Healthcare & Pharmaceuticals	39.7% Hospitality	51.4% Healthcare & Pharmaceuticals
32.4% Education	38.8% Healthcare & Pharmaceuticals	48.8% Insurance
31.2% Hospitality	36.2% Consulting	47.8% Consulting

PHASE ONE

BASELINE



Phase One

34.3% Initial Baseline Phishing Security Test Results

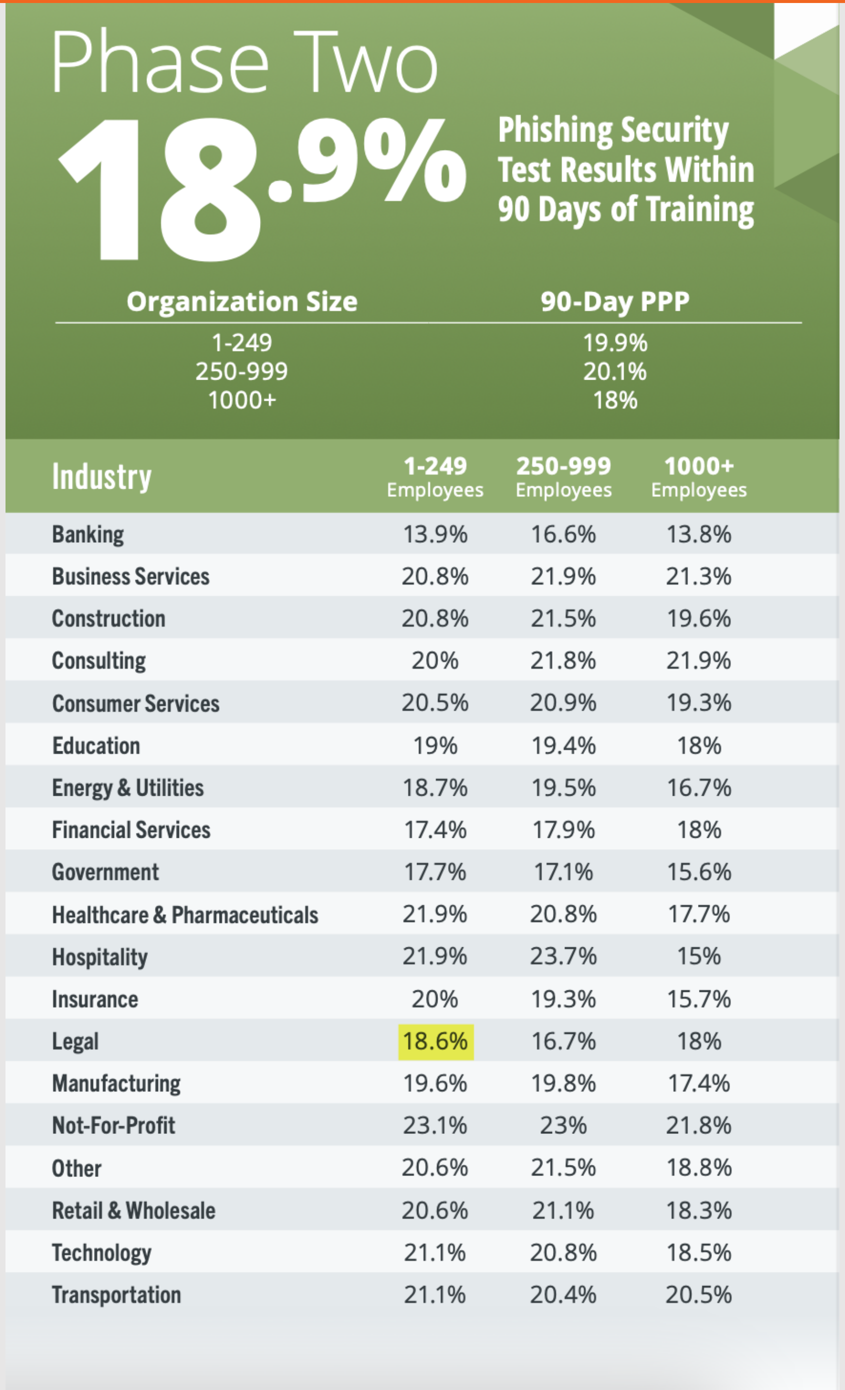
Organization Size	Initial PPP
1-249	28.7%
250-999	31.9%
1000+	37.5%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	27.8%	33.3%	42.3%
Business Services	26.7%	31.6%	33.2%
Construction	28.8%	35.0%	32%
Consulting	28.4%	36.2%	47%
Consumer Services	28.8%	31.2%	31.6%
Education	32.4%	31.2%	31.7%
Energy & Utilities	29.3%	33.3%	47.8%
Financial Services	28.1%	31%	41.6%
Government	27.9%	27.8%	28.6%
Healthcare & Pharmaceuticals	34.7%	38.8%	51.4%
Hospitality	31.2%	39.7%	31.8%
Insurance	28.6%	34.1%	48.8%
Legal	26.5%	29.2%	35.2%
Manufacturing	27.9%	31.6%	35.9%
Not-For-Profit	30.3%	33.9%	36.7%
Other	26.3%	28.9%	29.7%
Retail & Wholesale	30.7%	32%	42.4%
Technology	26.1%	30.3%	32.9%
Transportation	27%	28.6%	35.1%

KnowBe4
Human error. Conquered.

PHASE TWO

90 DAY



Phase Two

18.9% Phishing Security Test Results Within 90 Days of Training

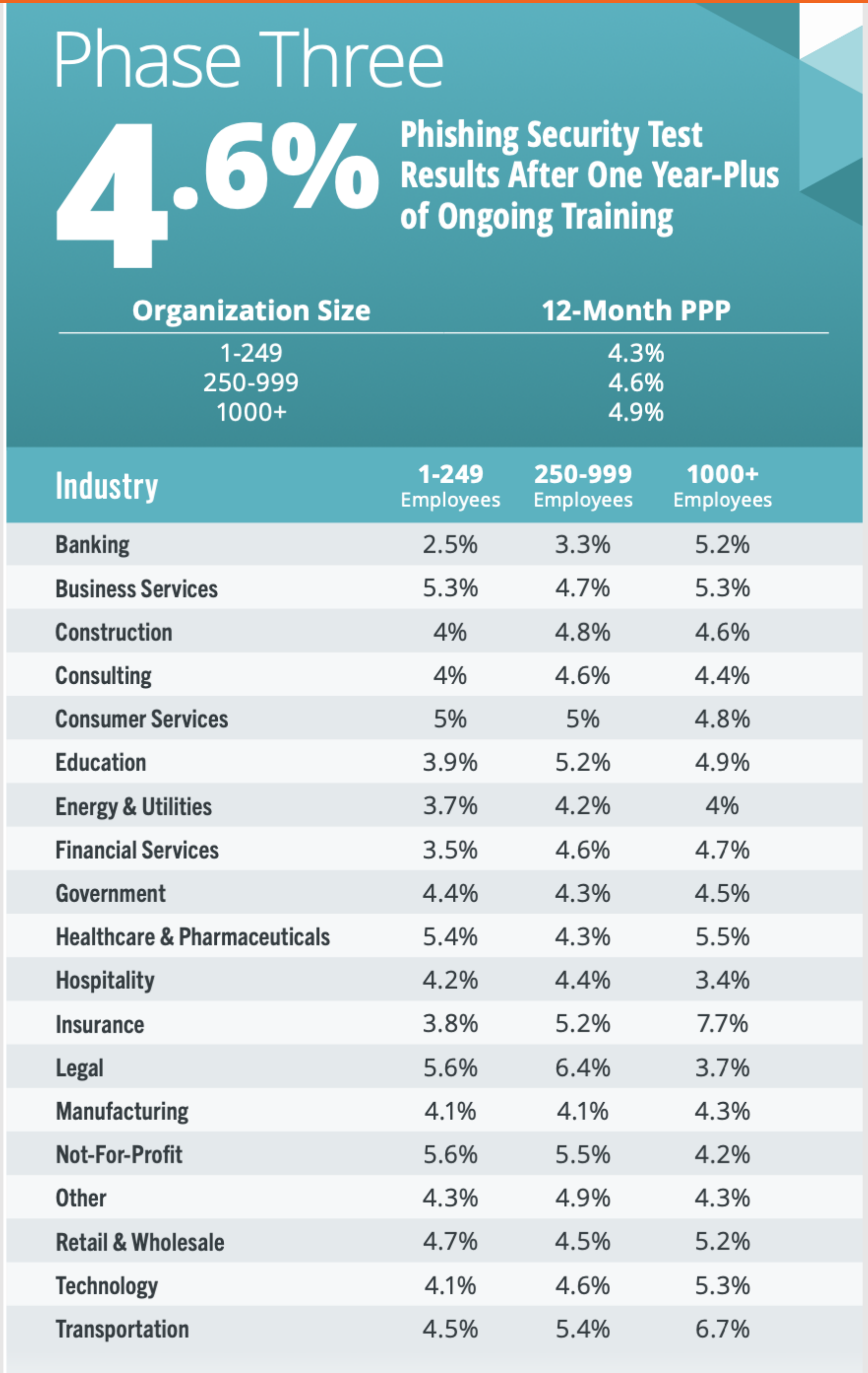
Organization Size	90-Day PPP
1-249	19.9%
250-999	20.1%
1000+	18%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	13.9%	16.6%	13.8%
Business Services	20.8%	21.9%	21.3%
Construction	20.8%	21.5%	19.6%
Consulting	20%	21.8%	21.9%
Consumer Services	20.5%	20.9%	19.3%
Education	19%	19.4%	18%
Energy & Utilities	18.7%	19.5%	16.7%
Financial Services	17.4%	17.9%	18%
Government	17.7%	17.1%	15.6%
Healthcare & Pharmaceuticals	21.9%	20.8%	17.7%
Hospitality	21.9%	23.7%	15%
Insurance	20%	19.3%	15.7%
Legal	18.6%	16.7%	18%
Manufacturing	19.6%	19.8%	17.4%
Not-For-Profit	23.1%	23%	21.8%
Other	20.6%	21.5%	18.8%
Retail & Wholesale	20.6%	21.1%	18.3%
Technology	21.1%	20.8%	18.5%
Transportation	21.1%	20.4%	20.5%

KnowBe4
Human error. Conquered.

PHASE THREE

12 MONTHS+



Phase Three

4.6% **Phishing Security Test Results After One Year-Plus of Ongoing Training**

Organization Size	12-Month PPP
1-249	4.3%
250-999	4.6%
1000+	4.9%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	2.5%	3.3%	5.2%
Business Services	5.3%	4.7%	5.3%
Construction	4%	4.8%	4.6%
Consulting	4%	4.6%	4.4%
Consumer Services	5%	5%	4.8%
Education	3.9%	5.2%	4.9%
Energy & Utilities	3.7%	4.2%	4%
Financial Services	3.5%	4.6%	4.7%
Government	4.4%	4.3%	4.5%
Healthcare & Pharmaceuticals	5.4%	4.3%	5.5%
Hospitality	4.2%	4.4%	3.4%
Insurance	3.8%	5.2%	7.7%
Legal	5.6%	6.4%	3.7%
Manufacturing	4.1%	4.1%	4.3%
Not-For-Profit	5.6%	5.5%	4.2%
Other	4.3%	4.9%	4.3%
Retail & Wholesale	4.7%	4.5%	5.2%
Technology	4.1%	4.6%	5.3%
Transportation	4.5%	5.4%	6.7%

KnowBe4
Human error. Conquered.

Agenda

1. The Threat Landscape
2. Phishing benchmark data by industry
3. Your Security Culture & "Human Firewall"

A security culture lives and breathes within every organization.

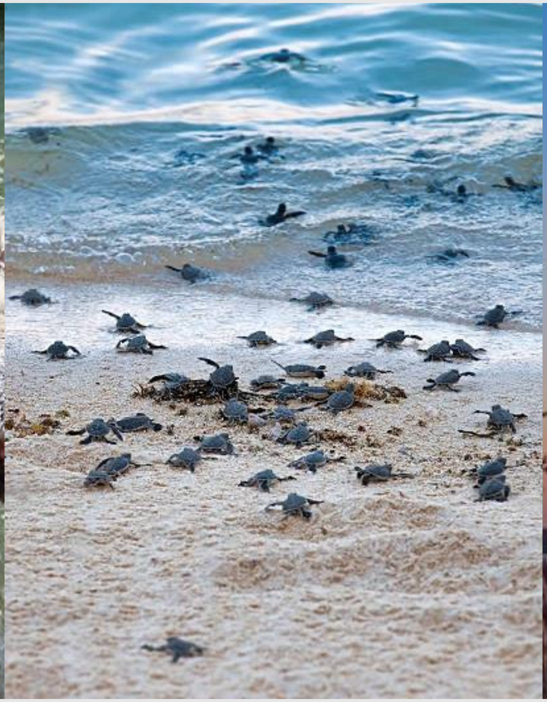
The question is how strong, intentional and sustainable is your security culture. And what do you need to do about it?

What if you educate?

What if everyone knew what to do?

KnowBe4
Human error. Conquered.

Instinctively…



Defining "Culture"

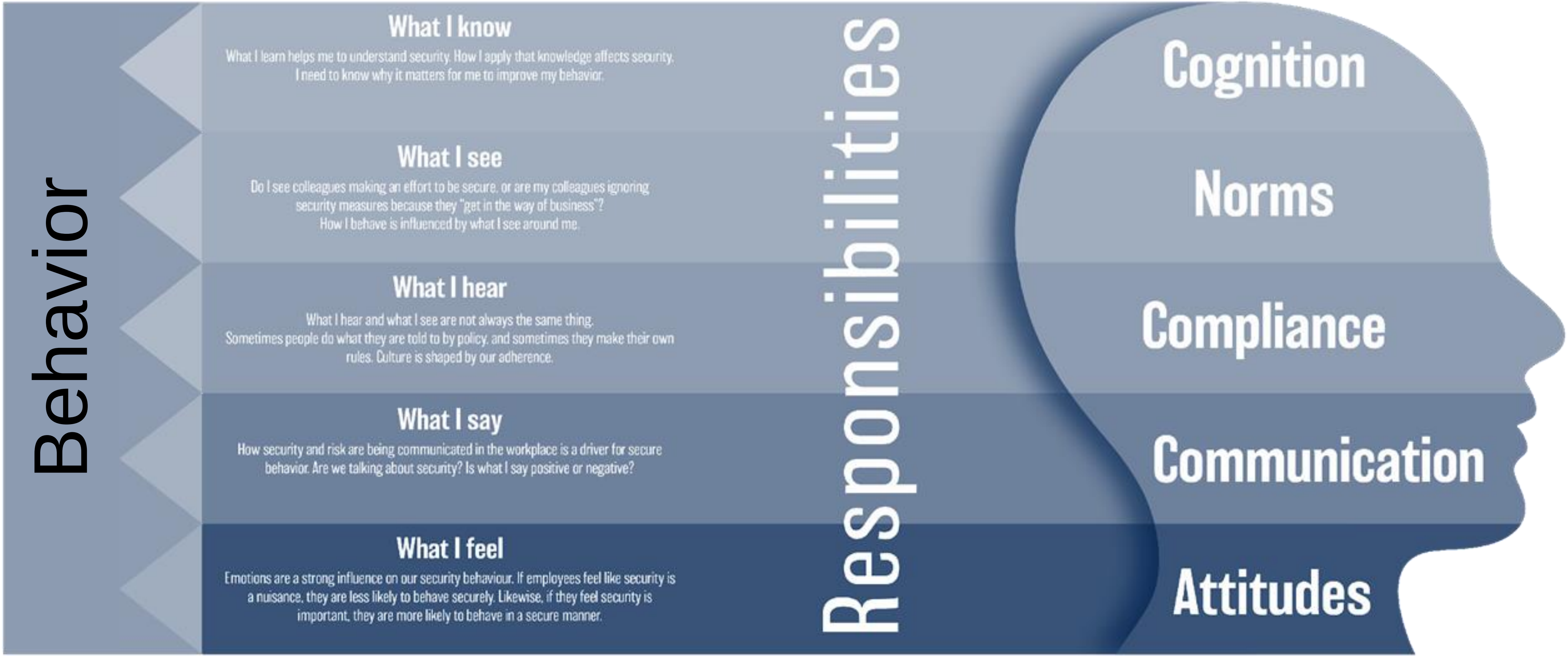
Organizational culture is not the sum of roles, processes and measurements; it is the sum of subconscious human behaviors that people repeat based on prior successes and collectively held beliefs.

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.

Security Culture:

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



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

Security Awareness and Secure Behavior are NOT the Same Thing

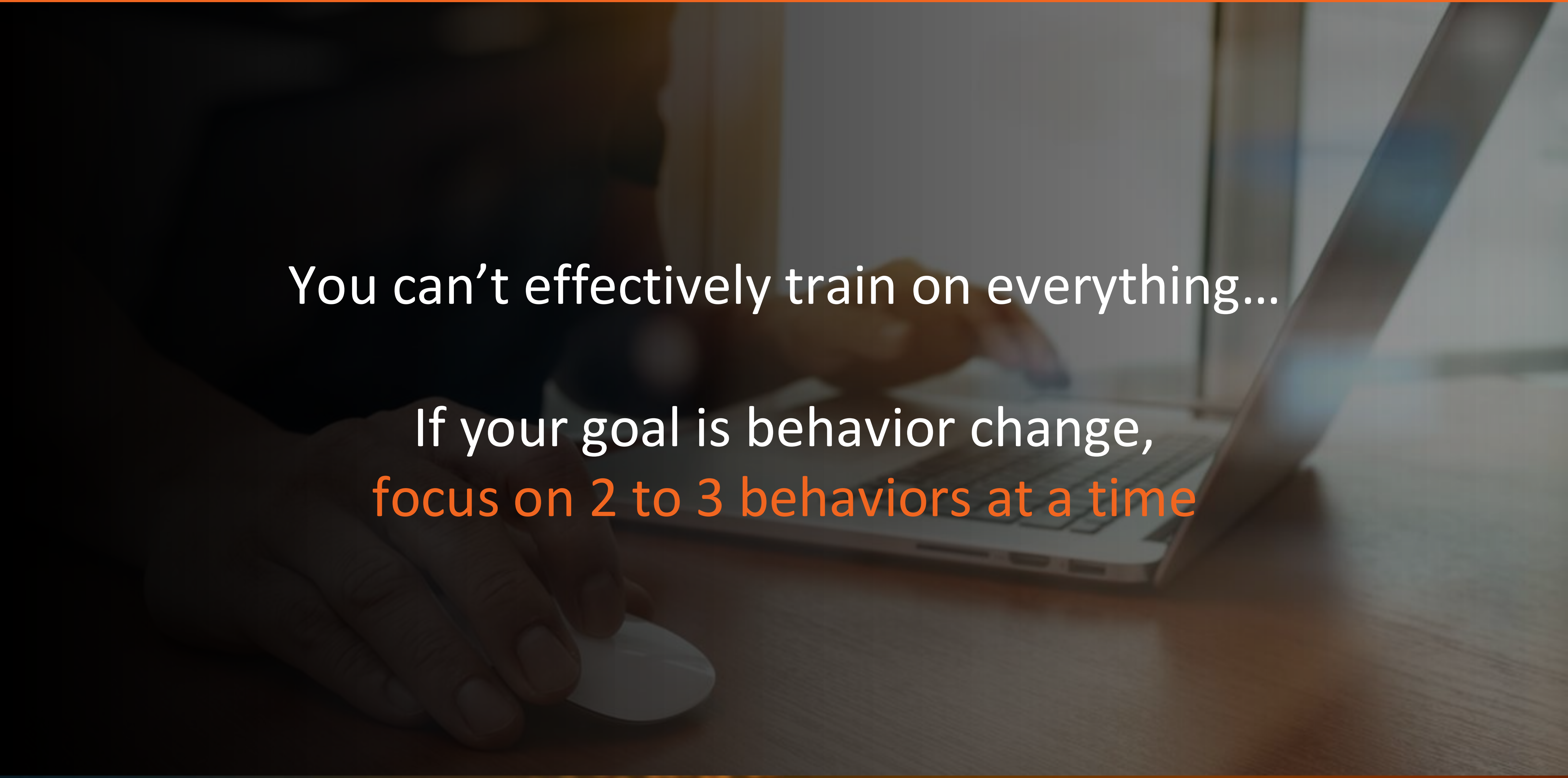
Just because I'm *aware* doesn't mean that I *care*.

KnowBe4
Human error. Conquered.

Your awareness program should not focus only on information delivery

Ask yourself:

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



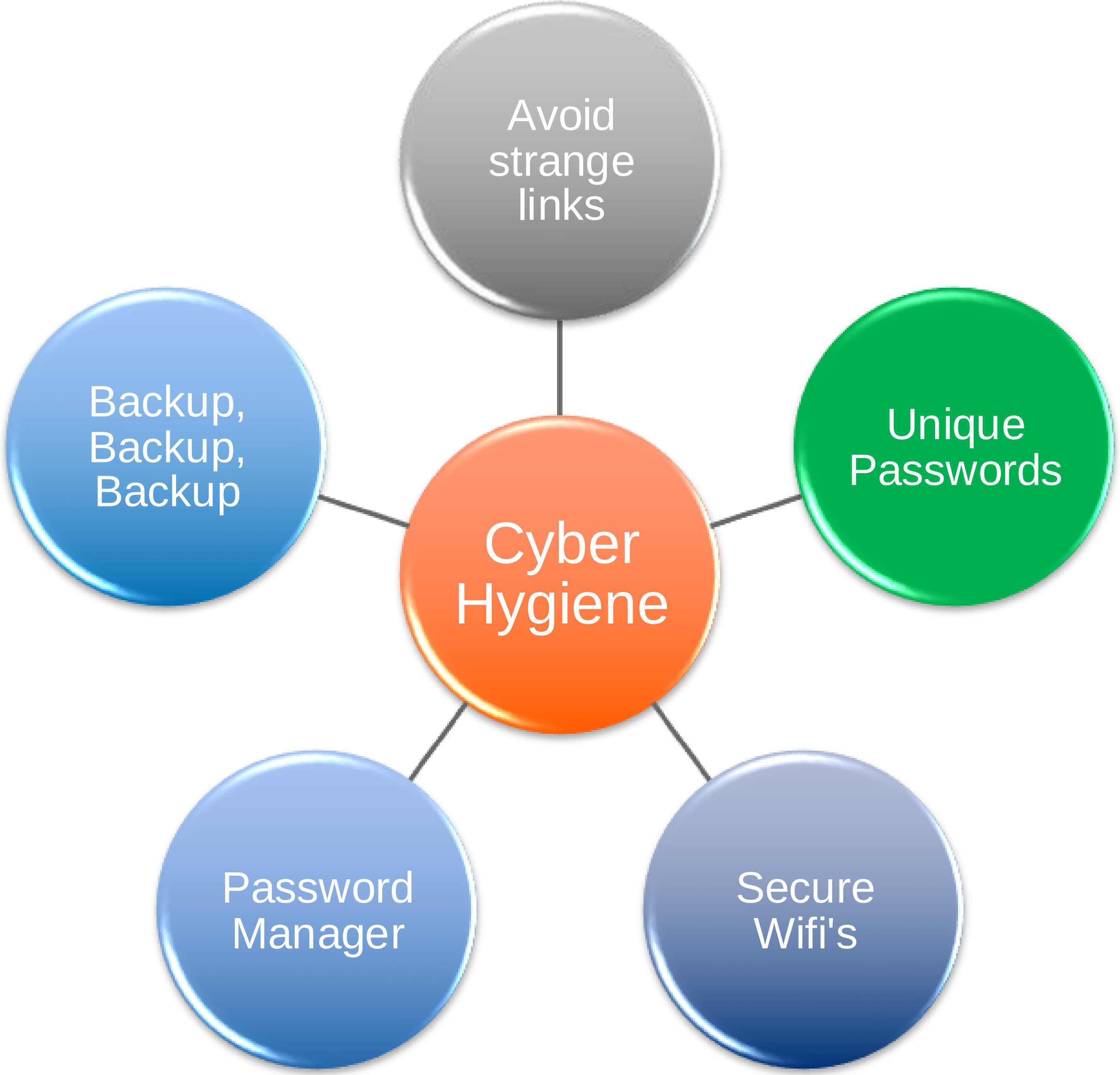
You can't effectively train on everything…

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

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.

Personal Cyber Hygiene


Cyber Hygiene

Avoid strange links

Unique Passwords

Secure Wifi's

Password Manager

Backup, Backup, Backup

5 Principles of Being a Human Firewall

01

Never make assumptions: Don’t draw your own conclusions.

02

Stay alert:

Keep your guard up.

03

Think critically: Slow down, verify, and think before you click.

04

See something? Say something: Immediately report incidents.

05

Follow policy, no matter what: Circumventing policy jeopardizes the company.

Final Thoughts

- Humans are the de-facto top choice for cybercriminals seeking to gain access into an organization.

Thank You

KnowBe4

Human error. Conquered.