ASMGi

Preventing Cyber Attacks with End User Security Awareness

Presented by ASMGi and KnowBe4

February 20, 2020

Today's Presenters – ***Preventing Cyber Attacks with End User Security Awareness***

Steve Roesing

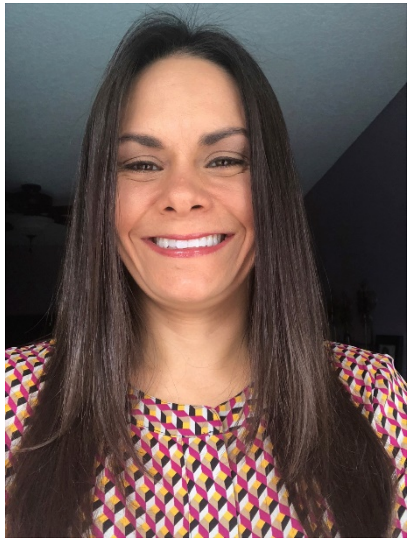
President, CEO, ASMGi

sroesing@asmgi.com

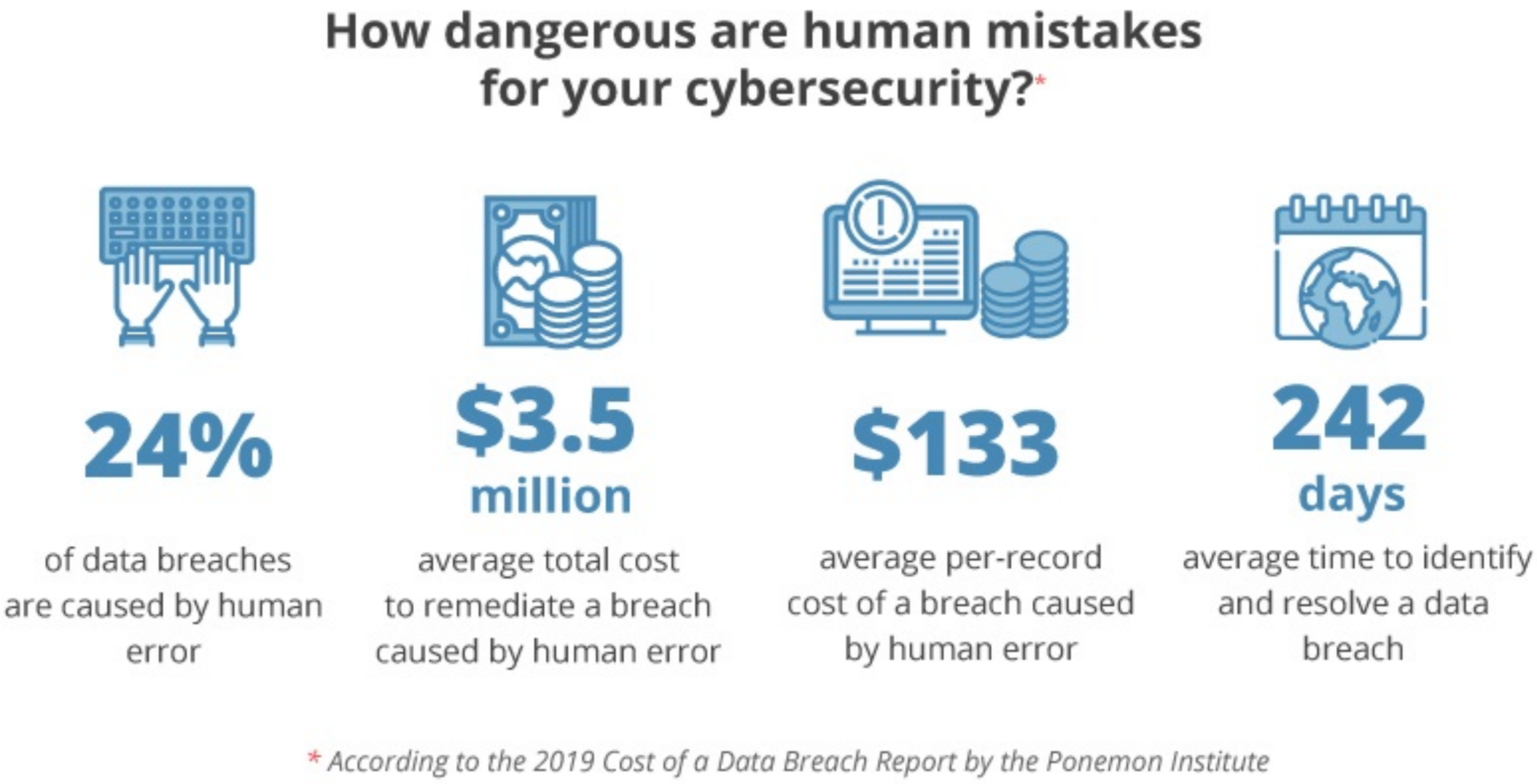
Cienne Blackburn

Channel Account Manager, KnowBe4

cienneb@knowbe4.com



Stats are staggering …



How dangerous are human mistakes for your cybersecurity?*

24%

of data breaches are caused by human error

$3.5 million

average total cost to remediate a breach caused by human error

$133

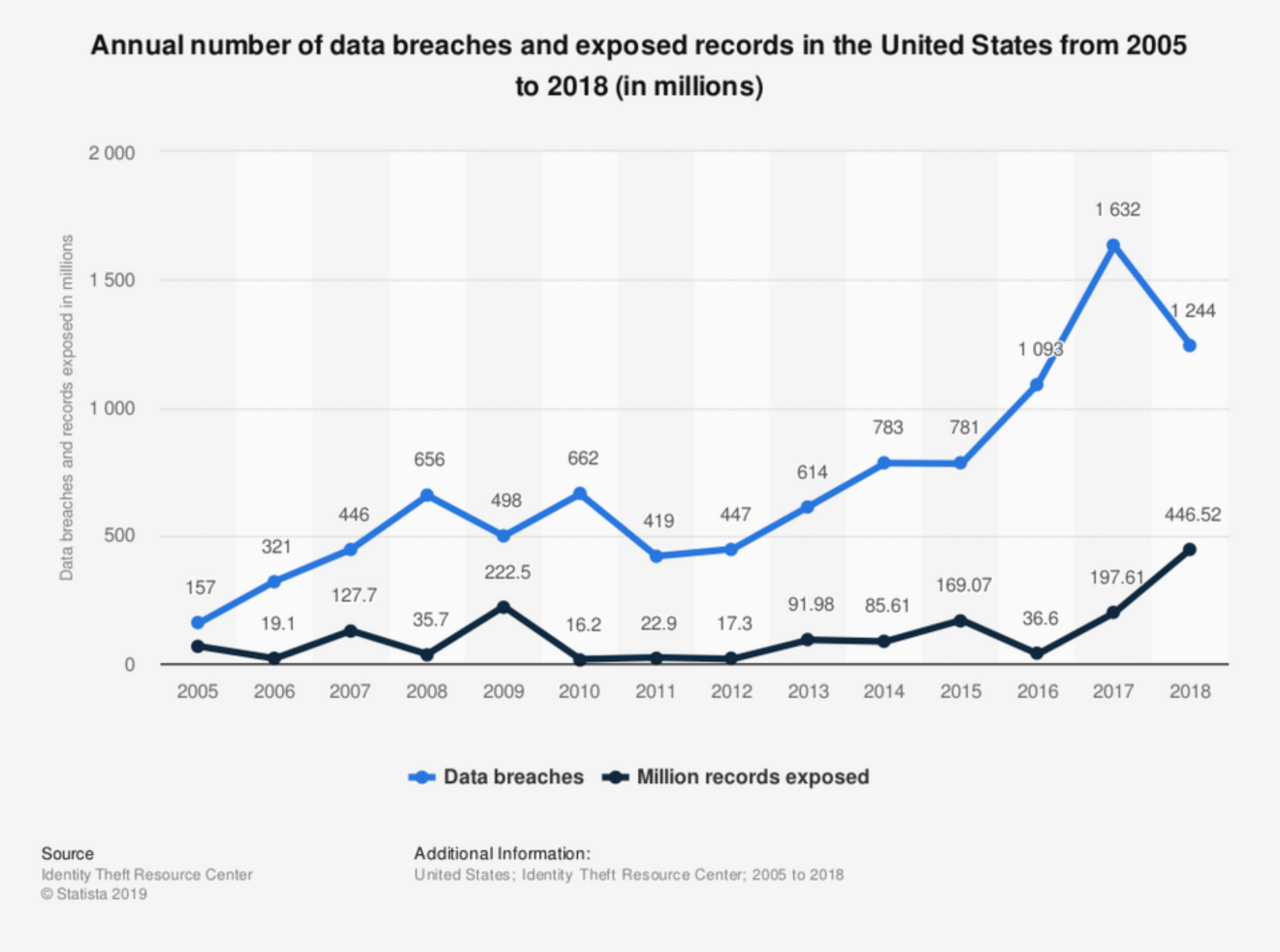
average per-record cost of a breach caused by human error

242 days

average time to identify and resolve a data breach

** According to the 2019 Cost of a Data Breach Report by the Ponemon Institute*

Stats are staggering …

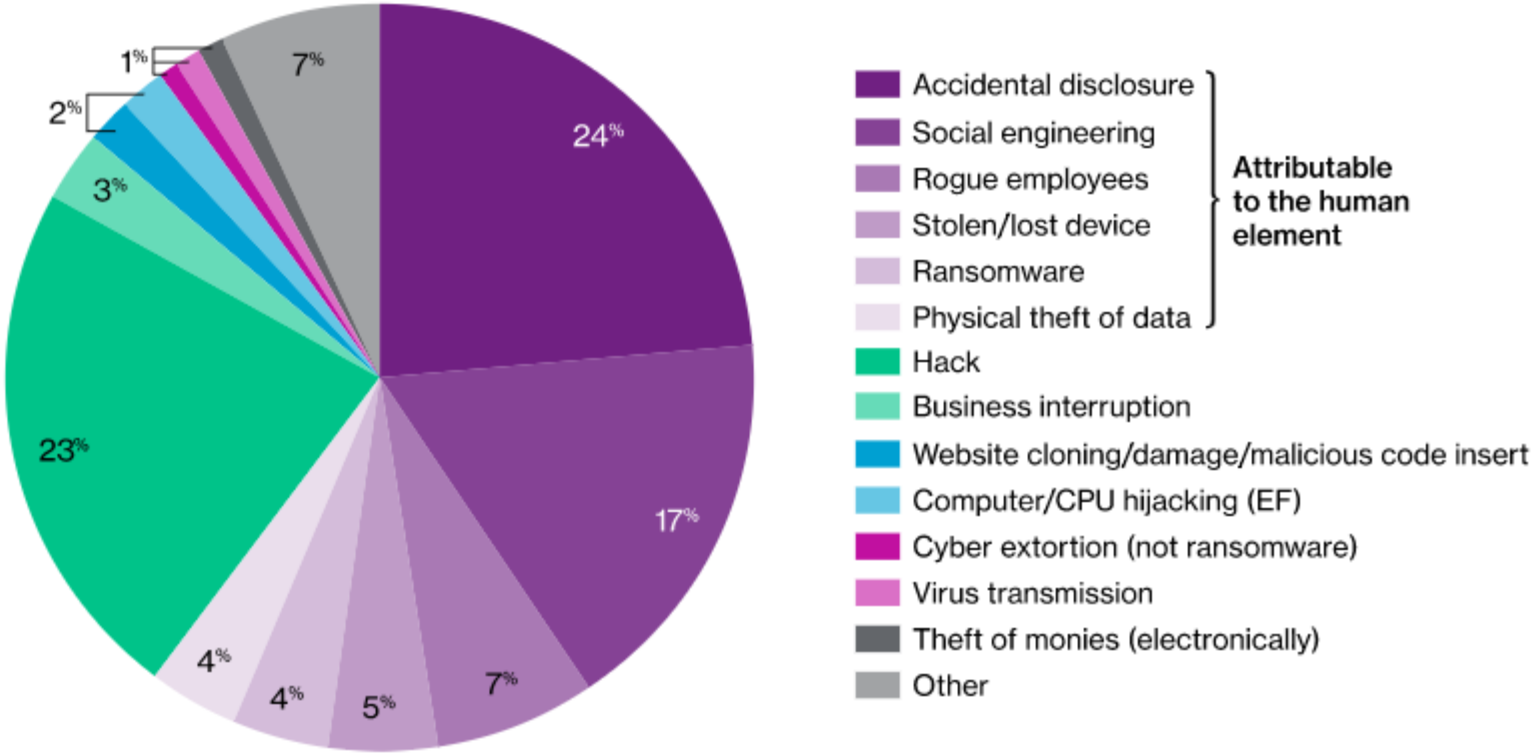


Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)

Source
Identity Theft Resource Center
© Statista 2019

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2018

Stats are staggering …



Looking at Historical Breach Data

Historical Breach Data annotated with CIS Controls

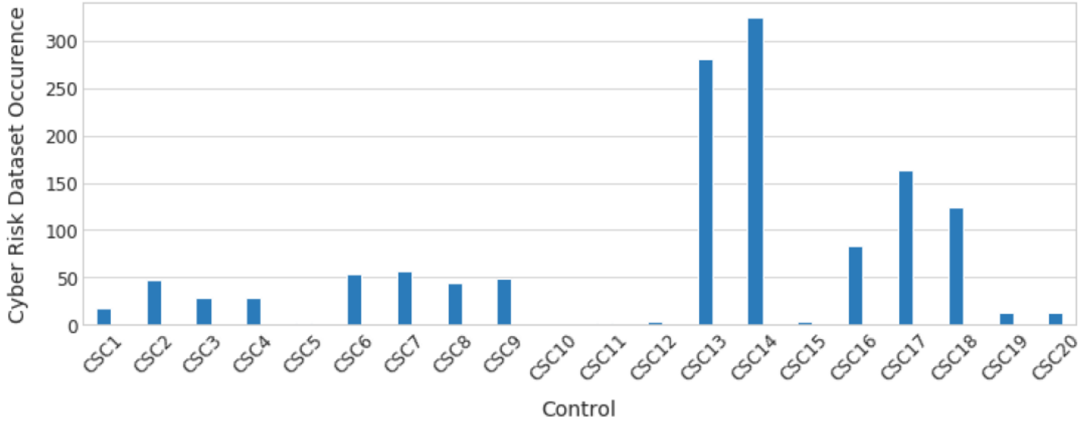


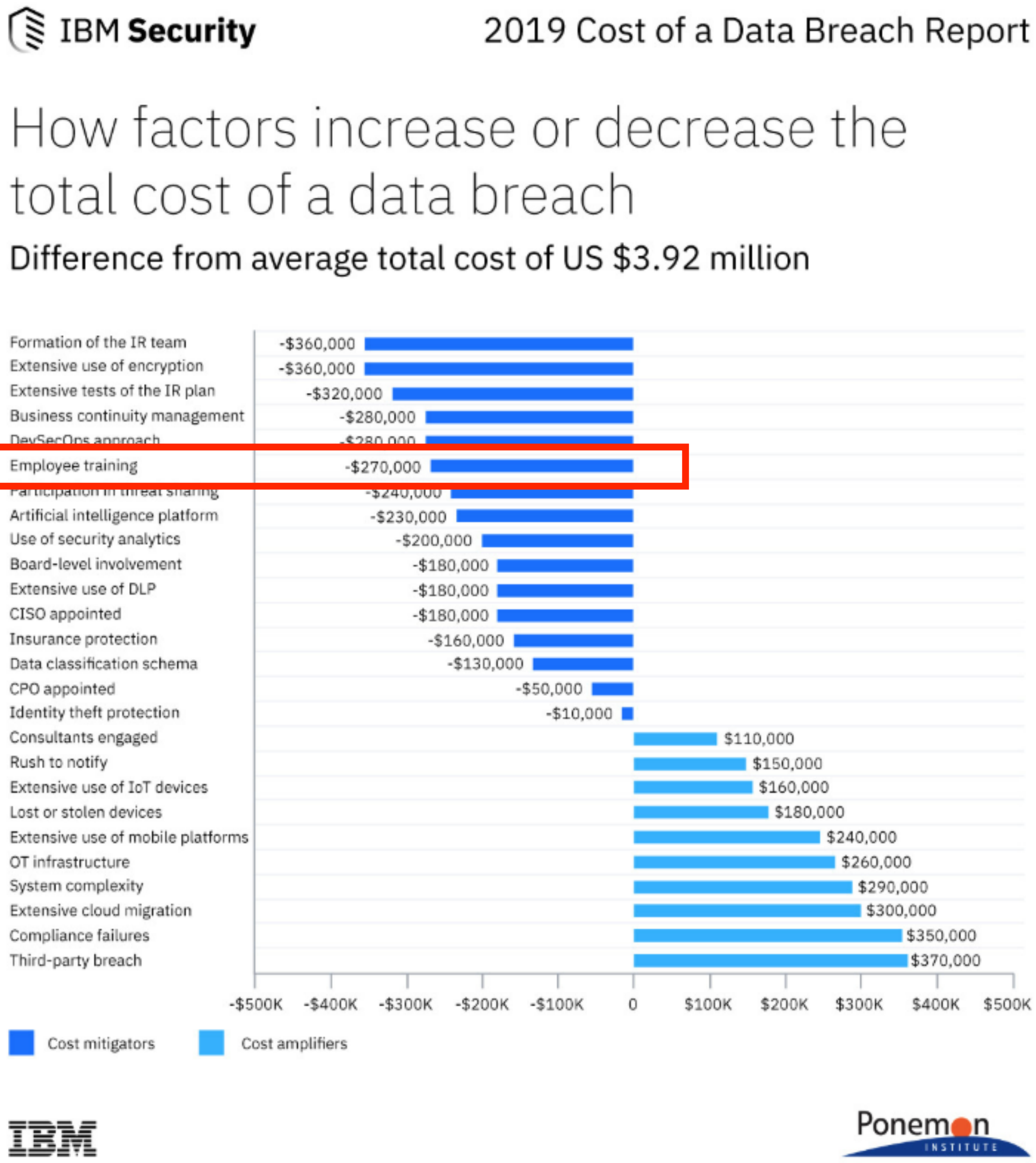
Figure 1: Shows the total number of times a CIS control could have prevented a cyber breach

The 3 most frequently affected controls from our analysis are:

CIS 14—Controlled Access Based on the Need to Know: This covers all the cases when the network was not properly segmented based on application and data sensitivity, e.g. cases when retailer's Point Of Sale (POS) devices were on the same network as regular employee endpoints. It also includes cases when shared folders were not properly protected with access controls and unauthorized people had access to sensitive data such as IP, PII, PHI, PFI, etc. Finally, scenarios such as unencrypted hard drives lost during transport by 3d parties, stolen unencrypted laptops, and disk drives.

CIS 13—Data Protection: This control covers all scenarios related to data stolen from undocumented or misplaced storage locations (laptops, network drives, 3d party cloud providers, etc.), data backups, legacy databases, and applications. Additionally, it includes cases when raw data in the clear text were exfiltrated without detection.

CIS 17—Implement a Security Awareness and Training Program: Covers all cases of fishing and more general cases when the attacker requested an employee to make some action such as making a wire transfer, sending a tax form or other sensitive information. Any unintentional disclosure of sensitive data to the attacker is included as well.



IBM Security

2019 Cost of a Data Breach Report

How factors increase or decrease the total cost of a data breach

Difference from average total cost of US $3.92 million

IBM

Ponemon INSTITUTE

How relevant is Security Awareness Training?

Compliance:

PCI-DSS: 12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

HIPAA: 164.308 (a)(5)(i) – Implement a security awareness and training program for all members of its workforce (including management).

CobiT: PO7.4 Personnel Training – Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational goals.

Frameworks:

NIST: NIST SP 800-50, Building an Information Technology Security Awareness and Training Program / NIST SP 800-53, AT 1-5: Security Awareness and Training Policy and Procedures, Security Awareness Training …

ISO/IEC 27001, 2: 8.2.2 – All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

CIS: Organizational Controls: CIS 17 –Implement a Security Awareness and Training Program

A Holistic Approach to Cyber Security

ASMGi

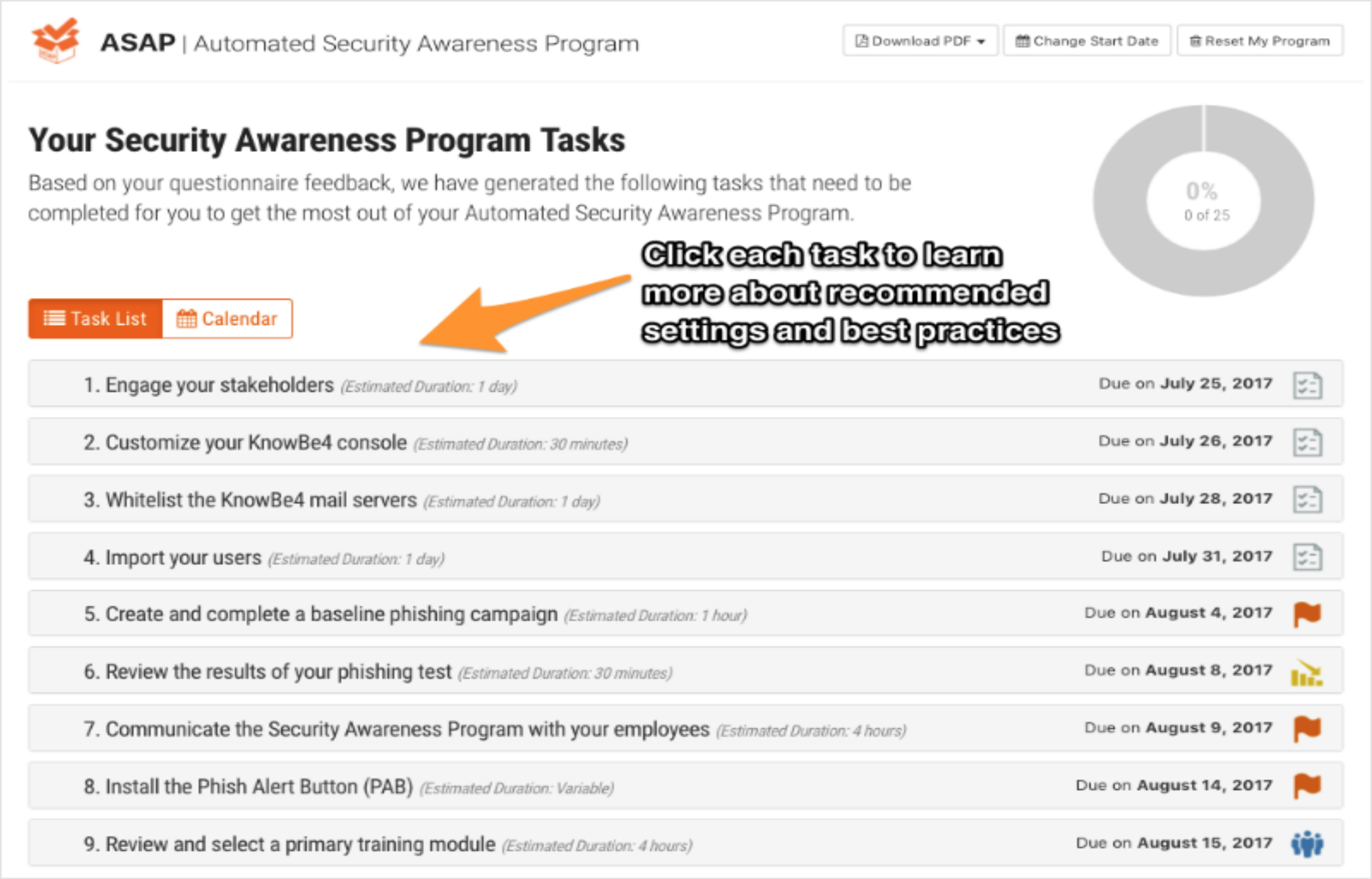
3 Pillars of a Total Solution

Program

Technology

Operations

Building a Security Awareness Program



ASAP | Automated Security Awareness Program

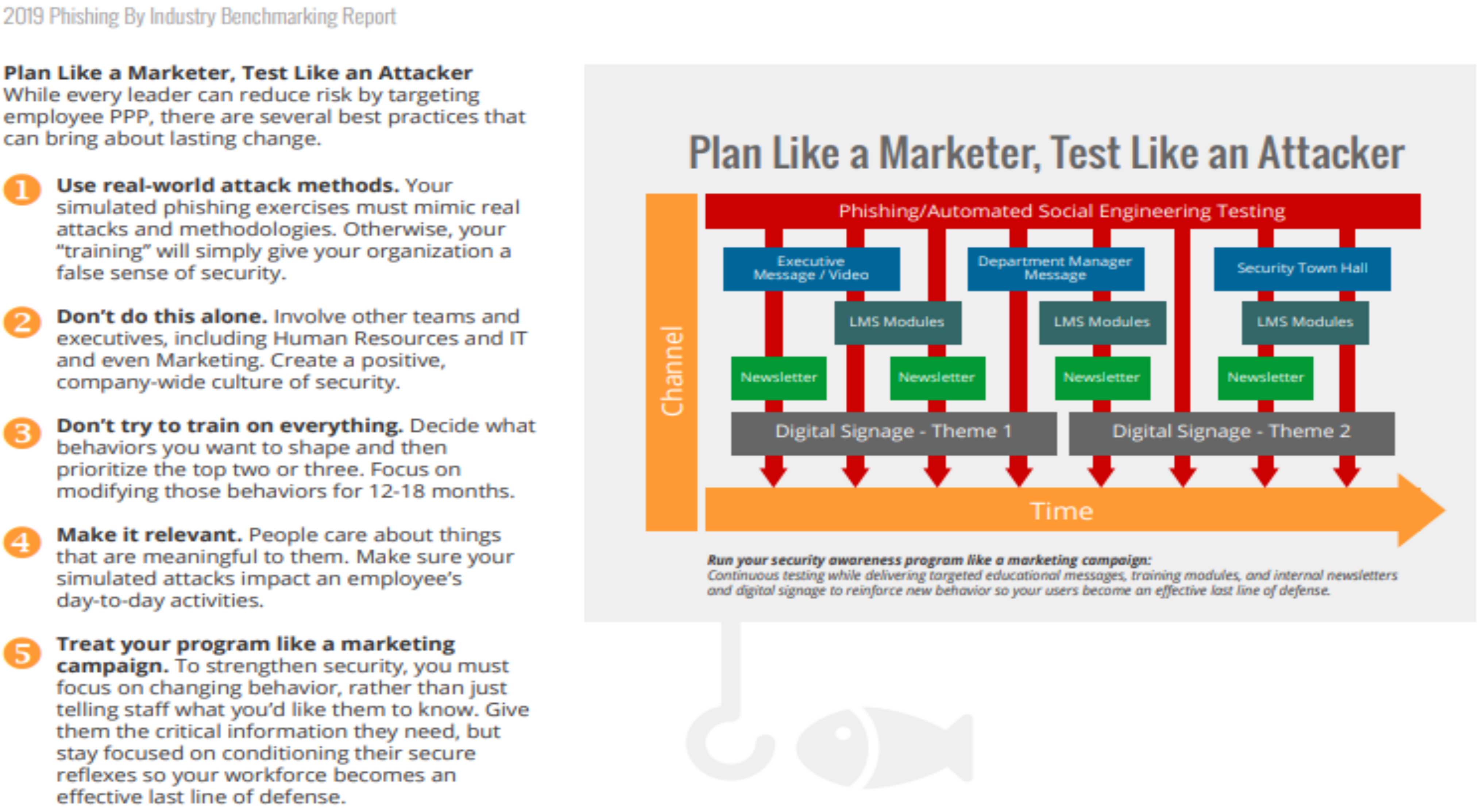
Your Security Awareness Program Tasks

Based on your questionnaire feedback, we have generated the following tasks that need to be completed for you to get the most out of your Automated Security Awareness Program.

Click each task to learn more about recommended settings and best practices

1. Engage your stakeholders *(Estimated Duration: 1 day)* — Due on **July 25, 2017**
2. Customize your KnowBe4 console *(Estimated Duration: 30 minutes)* — Due on **July 26, 2017**
3. Whitelist the KnowBe4 mail servers *(Estimated Duration: 1 day)* — Due on **July 28, 2017**
4. Import your users *(Estimated Duration: 1 day)* — Due on **July 31, 2017**
5. Create and complete a baseline phishing campaign *(Estimated Duration: 1 hour)* — Due on **August 4, 2017**
6. Review the results of your phishing test *(Estimated Duration: 30 minutes)* — Due on **August 8, 2017**
7. Communicate the Security Awareness Program with your employees *(Estimated Duration: 4 hours)* — Due on **August 9, 2017**
8. Install the Phish Alert Button (PAB) *(Estimated Duration: Variable)* — Due on **August 14, 2017**
9. Review and select a primary training module *(Estimated Duration: 4 hours)* — Due on **August 15, 2017**

Executing the plan …



2019 Phishing By Industry Benchmarking Report

Plan Like a Marketer, Test Like an Attacker
While every leader can reduce risk by targeting employee PPP, there are several best practices that can bring about lasting change.

1. **Use real-world attack methods.** Your simulated phishing exercises must mimic real attacks and methodologies. Otherwise, your "training" will simply give your organization a false sense of security.

2. **Don't do this alone.** Involve other teams and executives, including Human Resources and IT and even Marketing. Create a positive, company-wide culture of security.

3. **Don't try to train on everything.** Decide what behaviors you want to shape and then prioritize the top two or three. Focus on modifying those behaviors for 12-18 months.

4. **Make it relevant.** People care about things that are meaningful to them. Make sure your simulated attacks impact an employee's day-to-day activities.

5. **Treat your program like a marketing campaign.** To strengthen security, you must focus on changing behavior, rather than just telling staff what you'd like them to know. Give them the critical information they need, but stay focused on conditioning their secure reflexes so your workforce becomes an effective last line of defense.

Plan Like a Marketer, Test Like an Attacker

Phishing/Automated Social Engineering Testing
Channel
Executive Message / Video
Department Manager Message
Security Town Hall
LMS Modules
LMS Modules
LMS Modules
Newsletter
Newsletter
Newsletter
Newsletter
Digital Signage - Theme 1
Digital Signage - Theme 2
Time

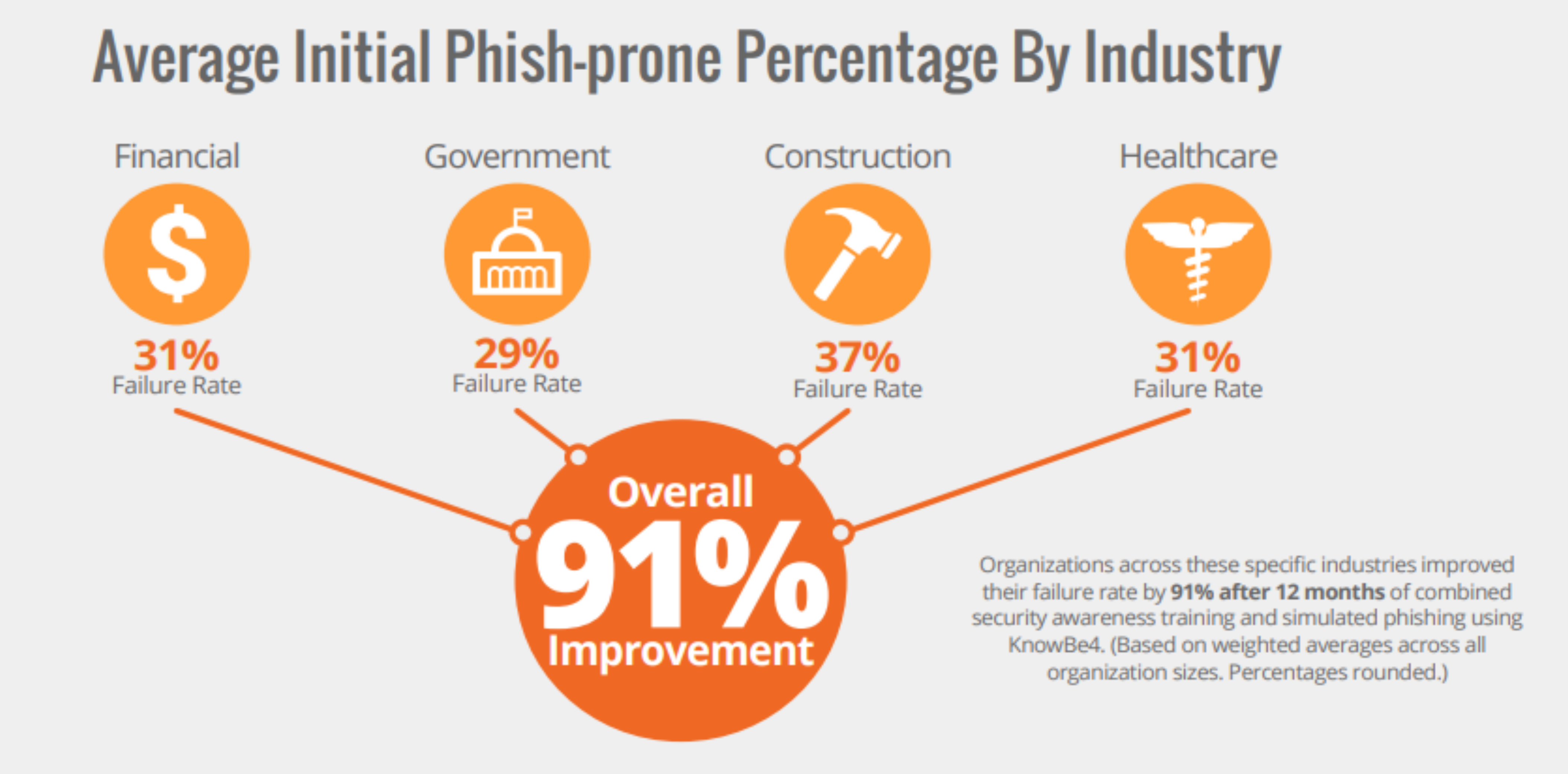
Run your security awareness program like a marketing campaign:
Continuous testing while delivering targeted educational messages, training modules, and internal newsletters and digital signage to reinforce new behavior so your users become an effective last line of defense.

Audience Poll …

How Many Times Per Year Do You Train Your Employees On Security?

A. None	10%
B. 1 – 2 times	40%
C. 3 – 5 times	35%
D. 6 – 12 times	10%
E. More than 12 times	5%

Results of training users…



Average Initial Phish-prone Percentage By Industry

Financial

31%
Failure Rate

Government

29%
Failure Rate

Construction

37%
Failure Rate

Healthcare

31%
Failure Rate

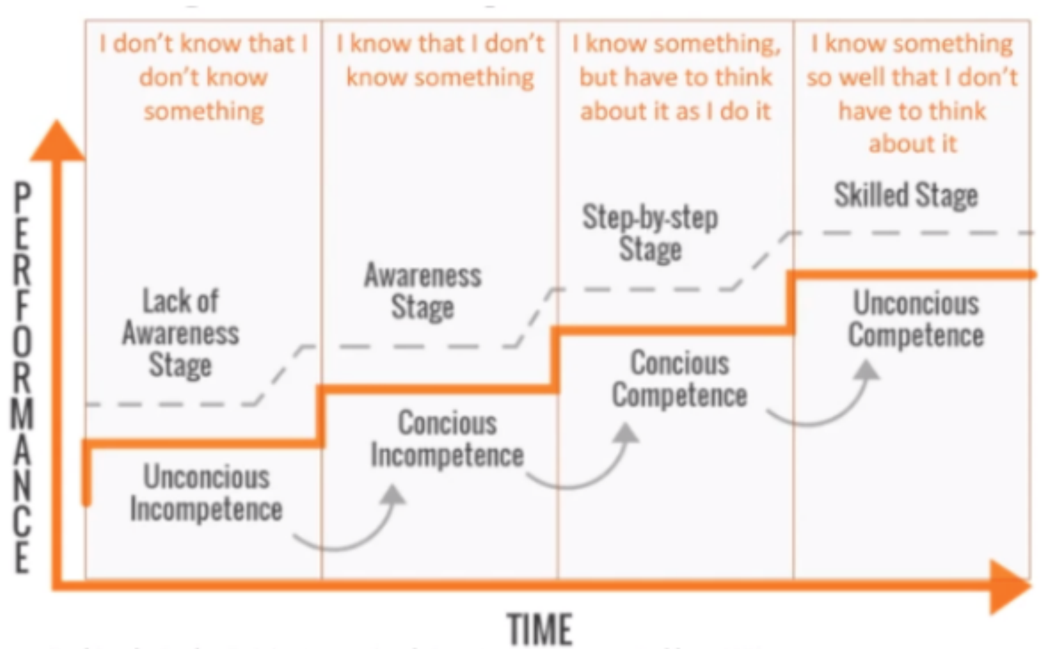
Overall
91%
Improvement

Organizations across these specific industries improved their failure rate by **91% after 12 months** of combined security awareness training and simulated phishing using KnowBe4. (Based on weighted averages across all organization sizes. Percentages rounded.)

Conscious Competence Ladder

The Four Stages of Competence

1. Lack of Awareness - Unconscious Incompetence or "I don't know that I don't know something." They are blissfully unaware and their behavior will reflect that.
2. Awareness - Conscious Incompetence or "I know that I don't know something." They now realize they don't have all the knowledge and tools they need. We can hope that will move them to the next stage.
3. Step-by-step - Conscious Competence or "I know something, but I have to think about it as I do it." They either need to access stored information or really intentionally weigh all the options then come to the right conclusion.
4. Skilled Stage - Unconscious Competence or "I know something so well that I don't have to think about it." This is where most of us are with pattern-based behaviors like driving, brushing our teeth, etc. At some point these things were difficult, and we can actually build up to this stage.


I don't know that I don't know something
I know that I don't know something
I know something, but have to think about it as I do it
I know something so well that I don't have to think about it
PERFORMANCE
Lack of Awareness Stage
Unconcious Incompetence
Awareness Stage
Concious Incompetence
Step-by-step Stage
Concious Competence
Skilled Stage
Unconcious Competence
TIME

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

KnowBe4
Human error. Conquered.

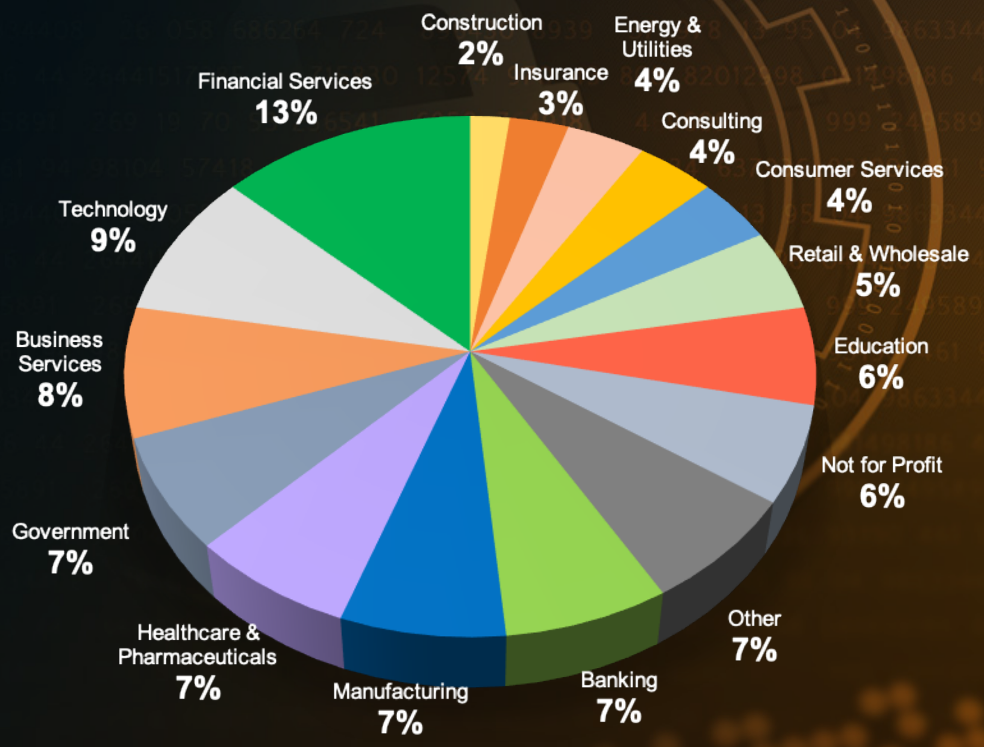
KnowBe4 Mission

Enable your employees to make smarter security decisions, every day

Over

30,000

Customers



About KnowBe4

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- KnowBe4 helps tens of thousands of organizations manage the ongoing problem of social engineering
- KnowBe4 provides an affordable, easy-to-use GRC tool that helps organizations cut down audit time and manage your compliance and risk projects faster than ever

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

AMERICA'S FASTEST-GROWING PRIVATE COMPANIES Inc. 500

Entrepreneur | cultureiQ TOP COMPANY CULTURES 2017

A staggering

91%

of successful data breaches start with a spear phishing attack

Users Are the Last Line of Defense

- **91%** of successful data breaches start with a spear phishing attack
- 30% of data breaches are caused by repeat offenders from within the organization

KnowBe4
Human error. Conquered.

The Costs of Breaches and Ransomware Attacks

$133K

- **34%** of businesses hit with malware take a **week or more** to regain access to their data
- The **average cost** of a ransomware attack on businesses is **$133,000**
- **75%** of companies infected with ransomware are running **up-to-date** endpoint protection

Source: Sophos 2018 and Kaspersky 2018

CEO Fraud and BEC Caused

$12.5B

In Identified Global Losses

BEC Attacks Are Growing

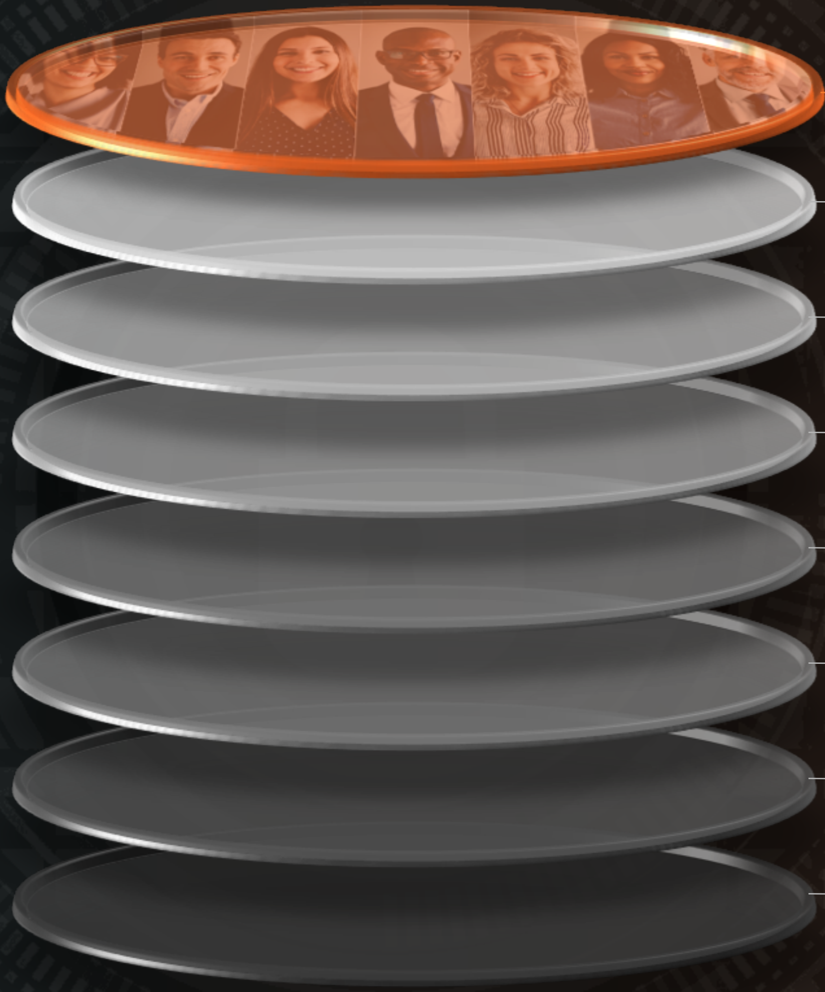
- **Business Email Compromise** (BEC) increased 136% in identified global exposed losses between Dec. 2016 and May 2018
- These attacks often contain **no links**, **no attachments** and no spelling or grammar errors.

Source: Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) 2018

People are a critical layer within the fabric of our Security Programs

KnowBe4 is the 8th Layer in Security

i.e. Building the **HUMAN FIREWALL**



8. Security Awareness Layer
7. Application Layer
6. Presentation Layer
5. Session Layer
4. Transportation Layer
3. Network Layer
2. Datalink Layer
1. Physical Layer

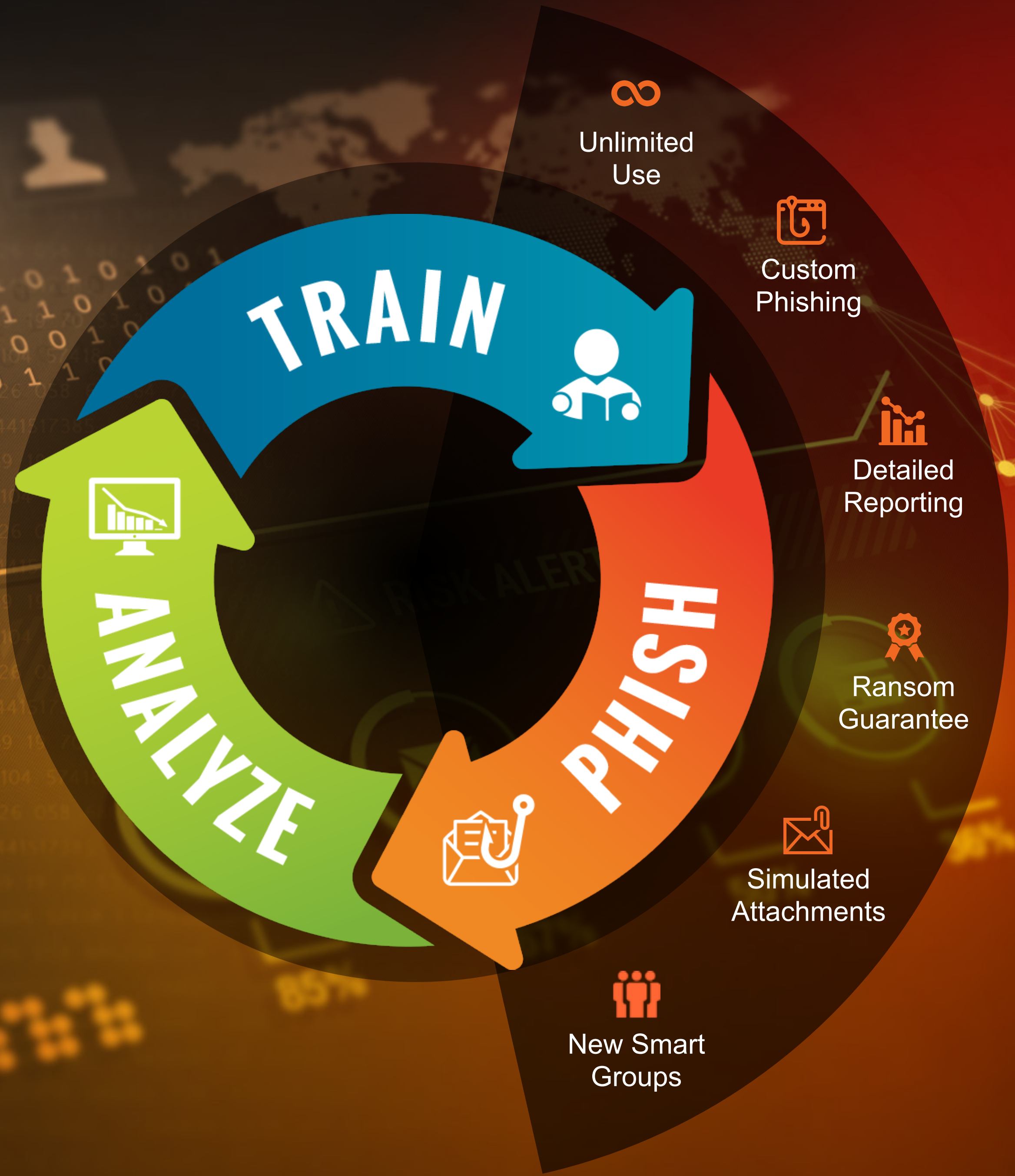
KnowBe4
Human error. Conquered.

Platform for Awareness Training and Testing

1 **Train Your Users**

2 **Phish Your Users**

3 **See the Results**



KnowBe4
Human error. Conquered.

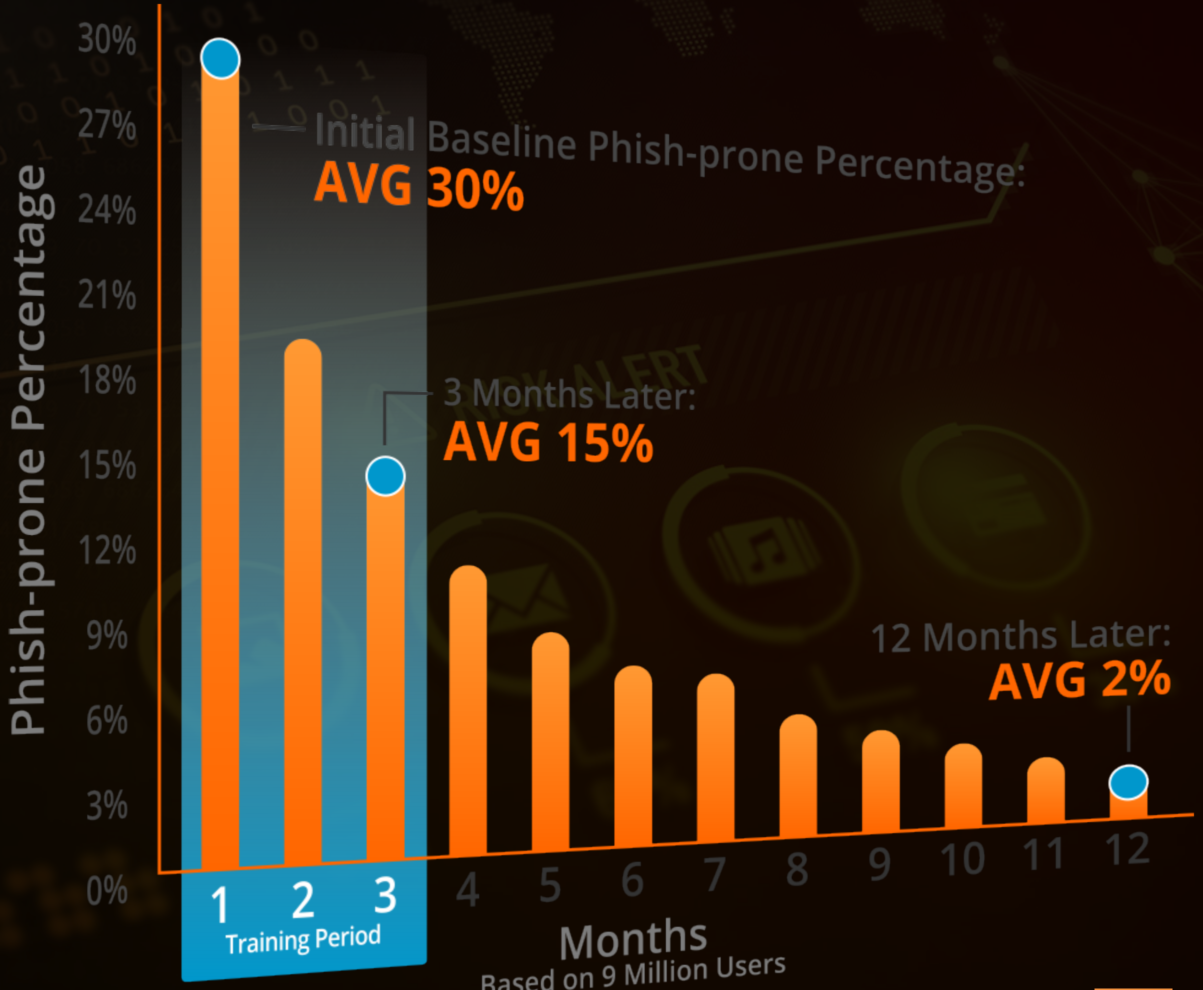
- Reduced Malware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

127% ROI

With a One-Month Payback

FORRESTER®

Generating Industry-Leading Results and ROI



KnowBe4
Human error. Conquered.

KnowBe4
Human error. Conquered.

Thank You

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

Special Offer for Attendees

ASMGi

QUESTIONS?

ASMGi

Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com