



**KnowBe4**  
Human error. Conquered.

# Cybersecurity: The Riskiest Landscape

*How to Make Your Security Awareness Program People-Centric*

## State of North Carolina Cyber Symposium - October 2022

Kathleen Gardner-VP Customer Relations | [kathleeng@knowbe4.com](mailto:kathleeng@knowbe4.com)

**DISCLAIMER:** This presentation contains simulated phishing attacks. The trade names/trademarks of third parties used in this presentation are solely for illustrative and educational purposes. The marks are property of their respective owners and the use or display of the marks does not imply any affiliation with, endorsement by, or association of any kind between such third parties and KnowBe4.

# Agenda

## Intro to KnowBe4

## Threat Intel

- Latest News - Mission Critical Times
- Cybersecurity is an everyone issue
- Latest Data & Research

## Engagement

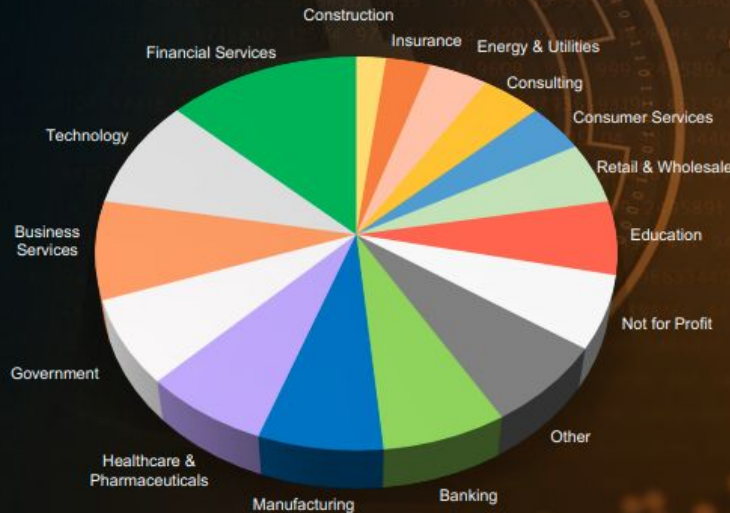
- Phishing Benchmarking 2022 Report
- Assessments - Awareness & Culture

## People-Centric Culture

- Building a Sustainable Security Culture
- Knowledge Starts in the Home
- Value Adds & Resources



Over  
**50,000**  
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, Norway, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil



# China Is Running Covert Operations That Could Seriously Overwhelm Us

Sept. 14, 2022



It's a different picture today. China has acquired global economic and diplomatic influence, enabling covert operations that extend well beyond traditional intelligence gathering, are growing in scale and threaten to overwhelm Western security agencies.

The U.S. and British domestic intelligence chiefs — the F.B.I. director, Christopher Wray, and the MI5 director general, Ken McCallum — signaled rising concern over this with an unprecedented joint news conference in July to warn of, as

Mr. Wray put it, a “breathtaking” Chinese effort to steal technology and economic intelligence and to influence foreign politics in Beijing’s favor. The pace was quickening, they said, with the number of MI5 investigations into suspected Chinese activity having increased sevenfold since 2018.

<https://www.nytimes.com/2022/09/14/opinion/international-world/china-espionage.html>

**The New York Times**



Brandon Wales, Executive Director of the Cybersecurity and Infrastructure Security Agency, in Washington last year.  
PHOTO: POOL/REUTERS

## Companies Should Treat Cyber Threats as Core Business Risk, U.S. Cyber Official Says

Brandon Wales, executive director of CISA, said boards need to push their companies to invest more on digital defense, adding that insurers and shareholders will be exerting pressure as well

- *“Cybersecurity needs to be driven at the board level - you don’t want to start thinking about cybersecurity after your network has been brought down by a ransomware operation”*
- *“Recently the US Securities & Exchange Commission proposed that companies be required to disclose detail on board members’ cyber expertise and how often the board addresses cybersecurity.”*
- *“Already critical infrastructure operators such as financial services firms and pipelines **MUST** comply with government-mandated cybersecurity requirements... **Over time that pressure will grow.**”*

THE WALL STREET JOURNAL.

<https://www.wsj.com/articles/companies-should-treat-cyber-threats-as-core-business-risk-u-s-cyber-official-say-s-11663701802>



# DEEP FAKES ARE HERE AND WE ARE NOT PREPARED...

**Q2 FBI Warning:**

“Deep Fakes Used to Apply for Remote Jobs in Tech”



**Business Identity  
Compromise (BIC)**



Metaphysic, an artificial intelligence company, teamed up with former “AGT” contestant Daniel Emmet to produce the deepfake

---

# 40%

Cyber #1 business risk, with 40% citing it as a serious risk

**“Cyber threats are no longer solely the domain of the CISO...”**

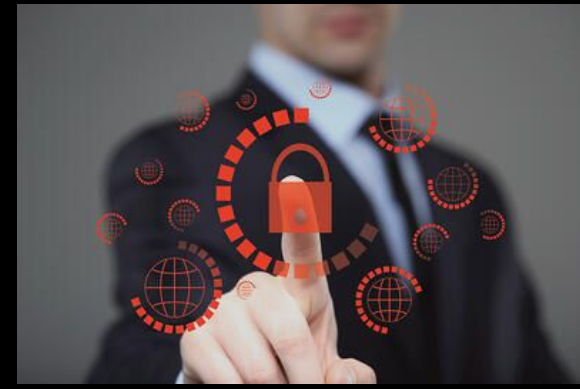
- View Cybersecurity as a broad business concern, not just an IT issue
- Educate your employees on cybersecurity practices
- For each new business unit, make sure there's a SA Plan
- Use data & intelligence to regularly measure your cyber risks

<https://www.pwc.com/us/en/library/pulse-survey/managing-business-risks.html>



**PwC Pulse Survey: Managing business risks**

Read time: 10 minutes



**Protect Your High Value Targets!**



# New eBook - Password Policy

## ***Recommended Password Policy Summary:***

*“Passwords and Password Policy comes down to risk acceptance and individual risk decisions. This whitepaper will make you a far better informed password and password policy implementer!”*

Roger Grimes

KnowBe4  
Human error. Conquered.

## What Your Password Policy Should Be

password:

<https://info.knowbe4.com/wp-password-policy-should-be>

# DBIR

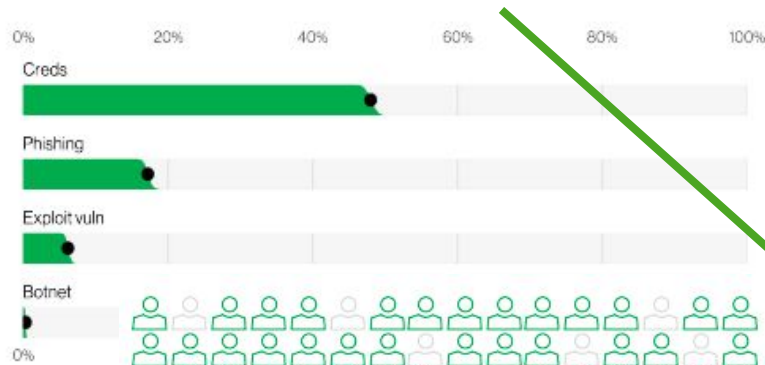
Data Breach Investigations Report

2008

2022

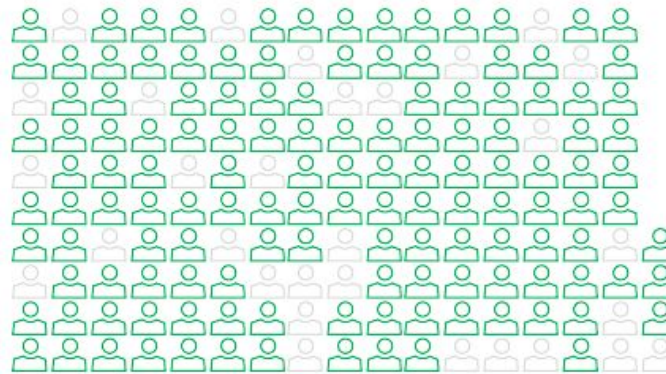


## Summary of findings



There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

Figure 5. Se



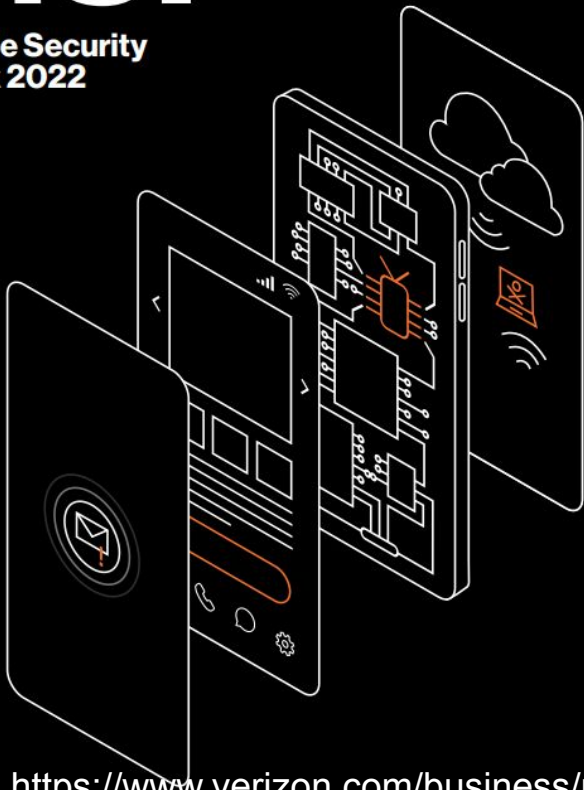
The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.

Figure 9. The human element in breaches (n=4,110)  
Each glyph represents 25 breaches.

**VERIZON'S** 2022 DBIR (15th Year)  
"82% of breaches involved the human element"

# MSI

Mobile Security  
Index 2022



<https://www.verizon.com/business/resources/reports/2022-msi-report.pdf>

X

## 79%

Nearly four-fifths (79%) of people admitted to using a work device for a personal task, such as checking personal email, shopping or streaming.<sup>16</sup>

## 48%

Nearly half of respondents said their organization didn't have an acceptable use policy in place.

Attacks are up—losses too.

## 45%

Close to half of the companies that we surveyed said they had suffered a compromise involving a mobile device in the past 12 months. Companies with a global presence were even more likely to have been affected. More than three in five (61%) had been hit, compared to 43% of organizations with only a local presence.

% Companies that suffered a mobile compromise

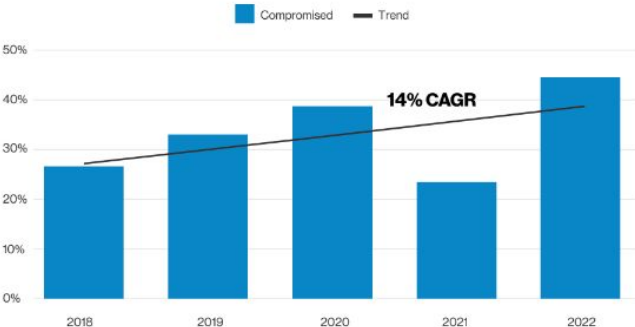


Figure 1. Percentage of respondents that admitted their company suffered a compromise that involved a mobile device and led to the loss of data or downtime. [n=601, 671, 876, 856, 632]

## RANSOMWARE

## 75%

Three-quarters of ransomware attacks start with email phishing.<sup>44</sup>



Percentage change in renewal premiums

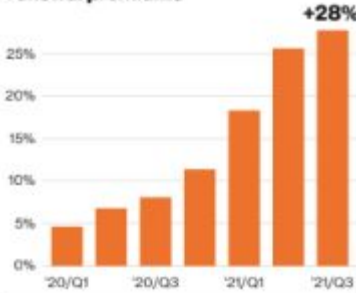


Figure 23. Increase in cyber insurance renewal premiums.<sup>45</sup>



# NEW! 2022 Phishing by Industry Benchmark Report

## EXECUTIVE TAKEAWAYS

### EXECUTIVE TAKEAWAYS

Security and risk management leaders need to understand that in order to favorably change overall security behaviors within their organizations, their programs must have:

- A clearly defined and communicated mandate
- A strong alignment with organizational security policies
- An active connection to overall security culture
- The full support of executives

Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.

<https://info.knowbe4.com/phishing-by-industry-benchmarking-report>



# Best Practice: Plan Like a Marketer, Test Like an Attacker...

## 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.

01

### 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.



02

### Don't do this alone

Involve other teams and executives, including Human Resources, IT and Compliance teams, and even Marketing. Create a positive, organization-wide culture of security.



03

### 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.



04

### 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.



05

### 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 security reflexes so your workforce becomes an effective last line of defense.

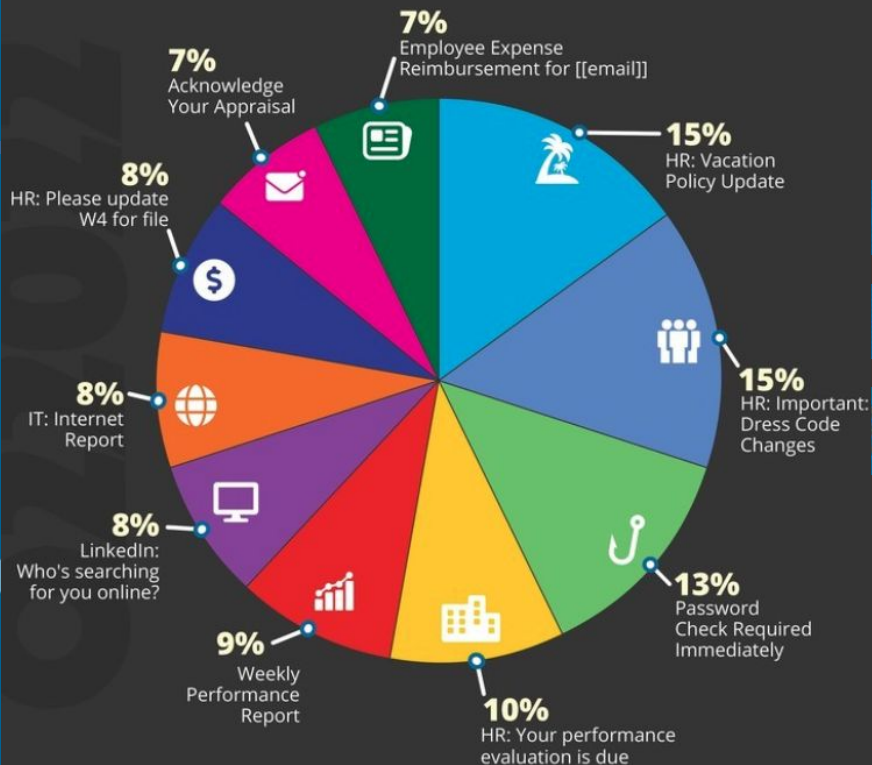


# TOP-CLICKED PHISHING TESTS Q2 2022

## COMMON "IN THE WILD" ATTACKS

- ✓ HR: Your performance evaluation is due
- ✓ Google: You were mentioned in a document: "Strategic Plan Draft"
- ✓ IT: Inventory Form
- ✓ Microsoft 365: Microsoft 365 has new password requirements
- ✓ Amazon: Balance paid on your seller account
- ✓ Xerox: New document was processed for [[email]]
- ✓ Zoom: [[manager\_name]] has sent you a message via Zoom Message Portal
- ✓ Facebook: Your recent Facebook login
- ✓ Your fax is pending for preview
- ✓ Money has been successfully withdrawn from your bank account

## TOP EMAIL SUBJECTS GLOBALLY



### KEY TAKEAWAY

Business phishing emails are the most clicked subject category across the world. These range from messages purporting to be from internal organizational departments, to external requests for information that convey a sense of urgency and entice users to take an action.

## TOP 5 ATTACK VECTORS:



LINK



SPOOFS  
DOMAIN



BRANDED

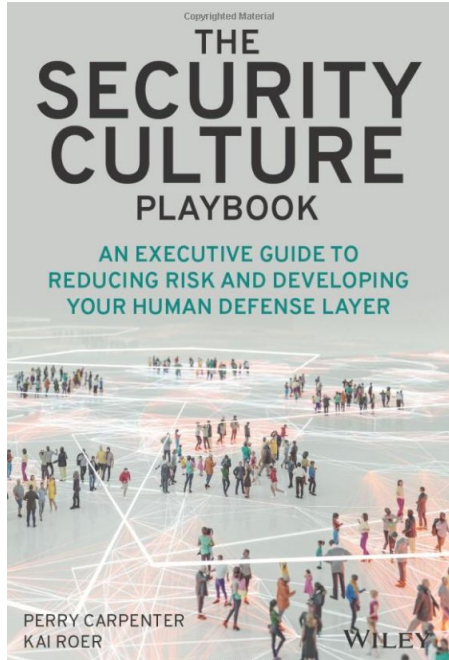


PDF  
ATTACH.



CREDENTIALS  
LANDING  
PAGE





**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?****



## 2022 Security Culture Survey

For Assessment: Security Culture Survey (SCS)

Your Security Culture Score

68

### Security Culture Index

90 - 100	Excellent
80 - 89	Good
70 - 79	Moderate
60 - 69	Mediocre
0 - 59	Poor

For more information on the Security Culture Index, [click here](#)

### Results by Dimension

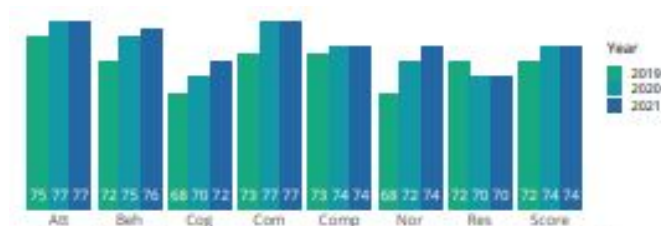
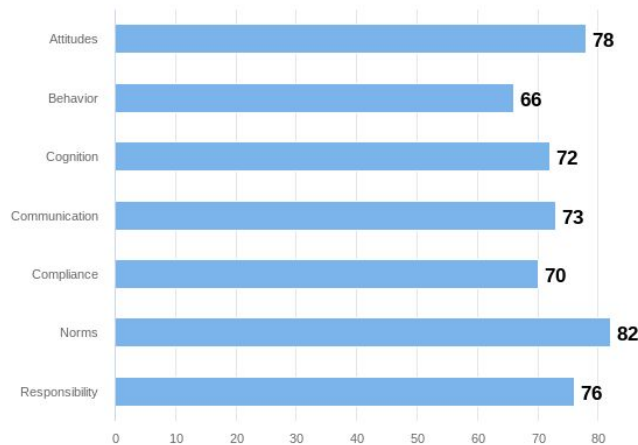


Figure 55: Trends as seen across the dimensions of security culture in Healthcare and Pharmaceuticals.

## 2022 Security Culture Report - Q2

### KnowBe4 Research

<https://www.knowbe4.com/organizational-cyber-security-culture-research-report>

# Gain Insight Into Where Your Organization Stands With the Security Culture Maturity Model

The Security Culture Maturity Model is an evidence-driven framework for understanding and benchmarking the current security-related maturity of an organization, industry vertical, region, or any measurable group.

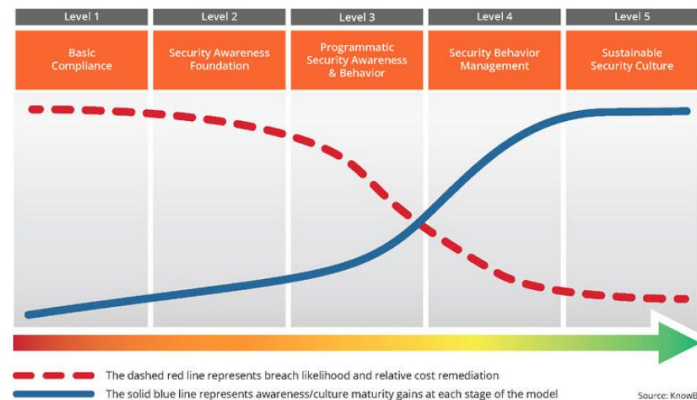
Get This Resource



KnowBe4 Research Model for Visualizing Security Culture Maturity

Our Security Culture Model is the industry's 1st maturity model specifically designed to measure security culture. This is science-backed research. When you think of Security Culture, it really comes down to human behaviors & human psychology - how do you create & sustain positive behaviors within your organization?

<https://www.knowbe4.com/security-culture-maturity-model>





# Building a Cyber Champions Advocacy Group

**Build an Army** - advocates spread across the organization in every department, region and country who can further translate and embed the security message within your organization.

**Ensure a constant stream** and reinforcement of security messaging moving through the organization. Your champions are culture carriers that act as evangelists to expand the message.

**Champions do not need to be security experts**, but they should be influencers in their areas, having the ability to engage their peers in ways that are relevant and meaningful.

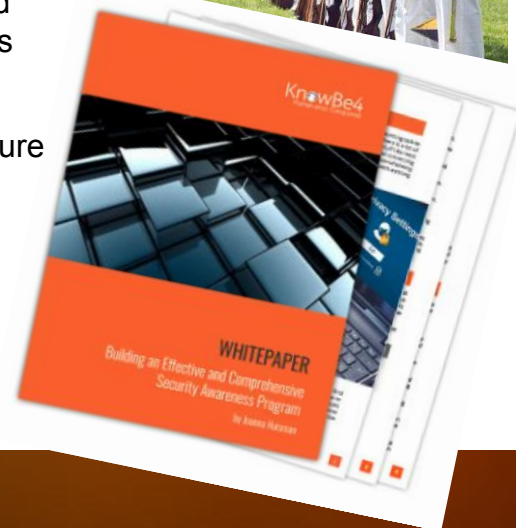
**Provide champions with the messaging content** and give them the liberty to translate and communicate that content in ways that are most effective for their audience. By localizing this messaging through champions, you now have a tremendous reach within the organization.

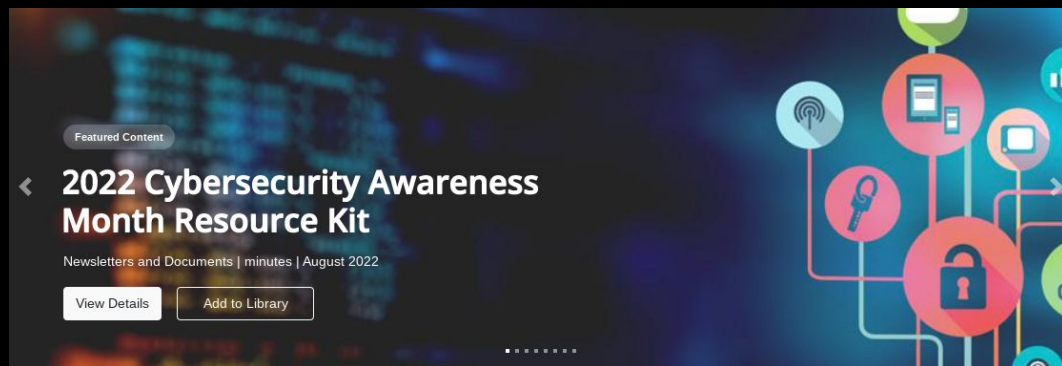
**Look for people who know how to be heard and drive change.** Champions drive the culture and share feedback on what is and is not working.

**Free WP: Building an Effective & Comprehensive Security Awareness Program**

*Joanna Huisman, KnowBe4 SVP Strategic Insights & Research*

<https://info.knowbe4.com/wp-building-effective-comprehensive-sat>





- **On-Demand Webinar**
- **Whitepaper**
- **Interactive Training Modules**
- **Interactive Games**
- **Newsletters**
- **Posters & Digital Signage**
- **Security Docs & Awareness Tips**

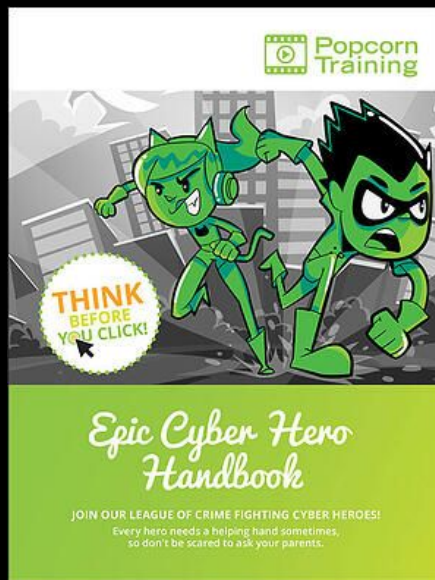
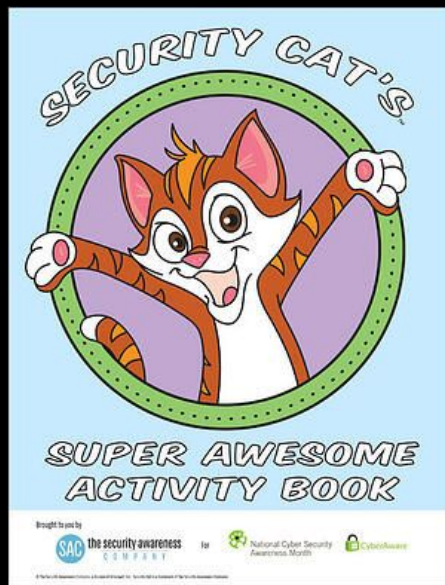
**CYBERSECURITY AWARENESS INTERACTIVE  
WEEKLY PLANNER WITH THEMES! AVAILABLE  
IN THE MOD STORE NOW!**

<https://www.knowbe4.com/cybersecurity-awareness-month-resource-kit>



**#CyberAware**

# KnowBe4 Children's Interactive Cybersecurity Activity Kit



<https://www.knowbe4.com/cybersecurity-activity-kit>



# Online Gaming Safety Tips for Adults, Kids, & Parents

JULY 14, 2022



- Block the Bullies
- Protect your Personal Information
- Play in Disguise
- Parental Controls



**NATIONAL  
CYBERSECURITY  
ALLIANCE**

<https://staysafeonline.org/programs/cybersecurity-awareness-month/>

## It's easy to stay safe online!



# Cyber Mindfulness - 8th Layer Insights

“why we think the things we think and do the things we do...using Cyber Mindfulness to reduce risk at your organization” <https://thecyberwire.com/podcasts/8th-layer-insights/21/transcript>

## 8<sup>th</sup> Layer Insights

Get ready for a deep dive into what cybersecurity professionals often refer to as the "8th Layer" of security: HUMANS. This podcast is a multidisciplinary exploration into how the complexities of human nature affect security and risk. Author, security researcher, and behavior science enthusiast Perry Carpenter taps experts for their insights and illumination. Topics include cybersecurity, psychology, behavior science, communication, leadership, and more.

### Subscribe



# Exec Takeaways for your SAC Program...

- Starts at the Top - Need to have Consistent & Enthusiastic Executive Support
- Clearly Defined and Communicated Mandate with a strong alignment to Corporate Security Policies
- Role Modeling - Lead your Employees Accordingly - Positive Reinforcement
- Engaging a Pro - Align with a vendor that can provide multiple types of content, versions and varieties that appeal to all different learning styles
- Think Like a Marketer! Monthly Simulated Phishing & Frequent Messaging in different formats (posters, digital signage, newsletters, short humorous 1min videos, etc.) to reinforce the message and create the secure culture and behaviors you are wanting to create
- Build an Advocates Group - “Cyber Champions” - that can help reinforce and expand the message in all areas of your organization



<https://insideman.knowbe4.com/>

# THE INSIDE MAN



FESTIVAL DE CANNES

[HOME](#)

[INSIDE THE EPISODES](#)

[MEET THE CHARACTERS](#)


[AWARDS & REVIEWS](#)

[BEHIND THE SCENES](#)

## THE INSIDE MAN SEASON 4 NOW AVAILABLE

[Watch The Trailer](#)





# Thank You!

# Q&A

**KnowBe4**  
Human error. Conquered.

**Know more about KnowBe4.**

**knowbe4.com**

**855.566.9234**