Cybercriminals don't care about this and use them anyway to trick you….

This presentation may contain 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.

American Gear Manufacturers Association®

AGMA EMERGING TECHNOLOGY SPECIAL PRESENTATION

June 20, 2024

5 Ways to Reduce Risk of an Organization Being Hacked

James McQuiggan, CISSP, SACP
Security Awareness Advocate
KnowBe4

Please make sure to have your microphone on mute. We will begin shortly.

WEBINAR SERIES SPONSORS

Gleason

REISHAUER
Gear Grinding Technology

KnowBe4
Human error. Conquered.

5 Ways to Reduce Risk of an Organization Being Hacked

James R. McQuiggan, SACP, CISSP
Security Awareness Advocate

KnowBe4
Human error. Conquered.

5 Ways to Be Hacked

James R. McQuiggan, SACP, CISSP
Security Awareness Advocate

What Is Common About These Logos?

Verizon Data Breach Incident Report

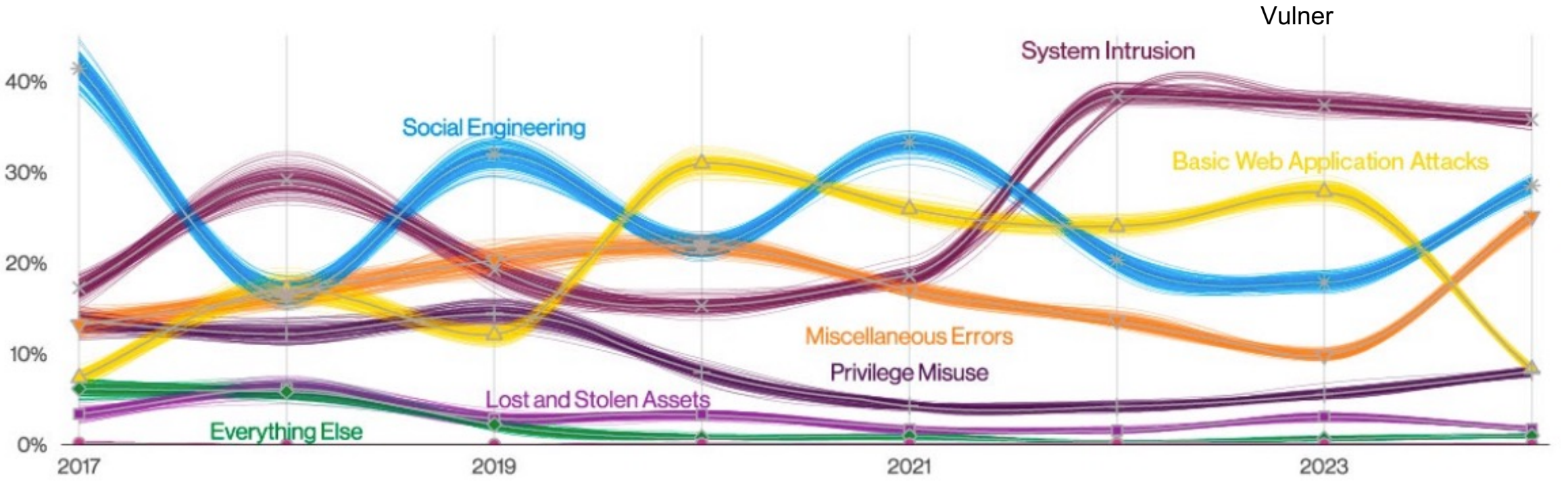
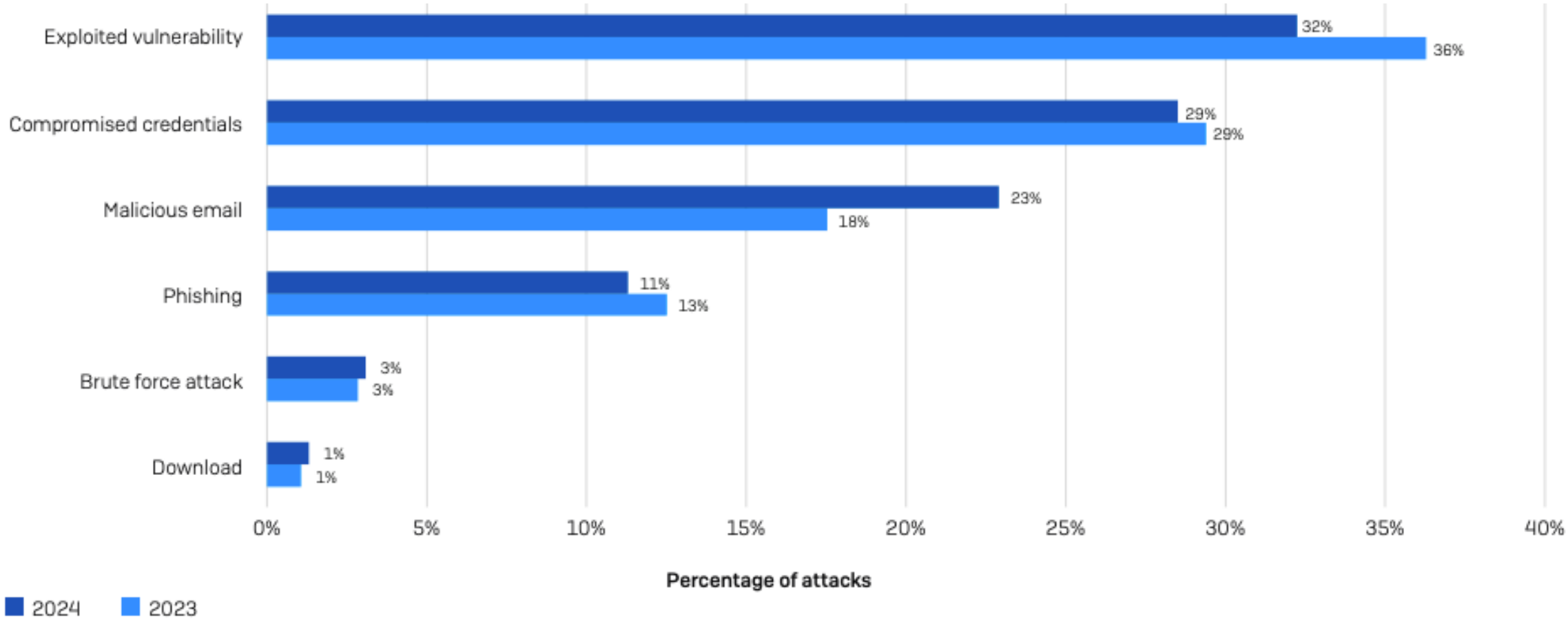


Figure 27. Patterns over time in breaches

System Intrusion, Social Engineering, Misc. Error, Privilege Misuse, Lost Stolen Assets, Everything Else

Attack Vectors For Ransomware



Source: Sophos – The State of Ransomware

CYBERATTACKERS USE SEVERAL TECHNIQUES TO PERPETUATE ATTACKS.

Lockton Claims (Insurance)

Common Attack Vectors

Exploited Vulnerabilities

Brute Force Attack

Compromised Credentials

Malicious Email

Phishing

James R. McQuiggan, CISSP,SACP

Security Awareness Advocate, KnowBe4 Inc.

Producer, Security Masterminds Podcast

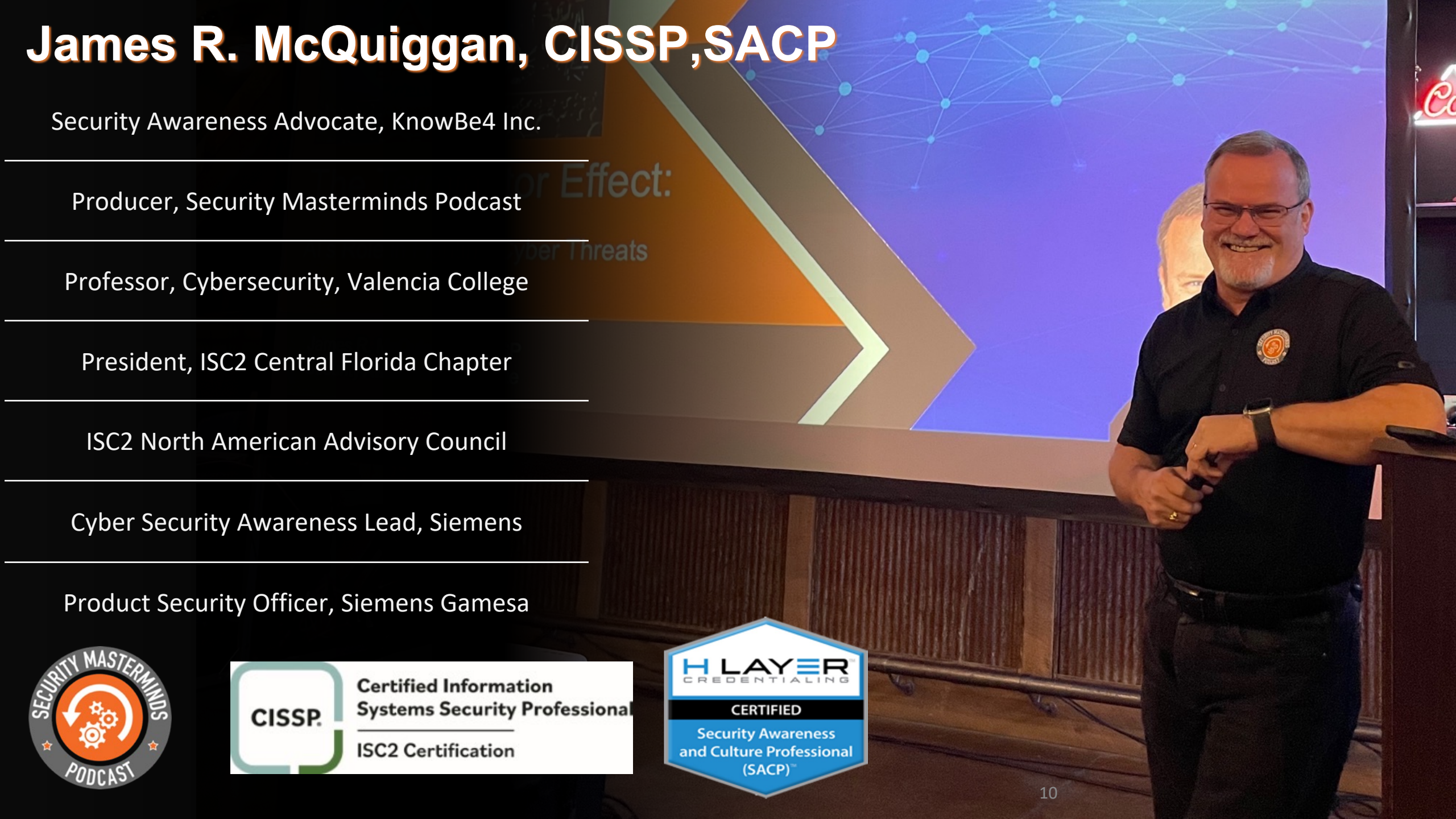
Professor, Cybersecurity, Valencia College

President, ISC2 Central Florida Chapter

ISC2 North American Advisory Council

Cyber Security Awareness Lead, Siemens

Product Security Officer, Siemens Gamesa



KnowBe4

About KnowBe4

- 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 ™

Our mission

To help organizations manage the ongoing problem of social engineering

We do this by

Enabling employees to make smarter security decisions everyday

I figured out Forrest Gump's password

1-Forrest-1

Exploited Vulnerabilities

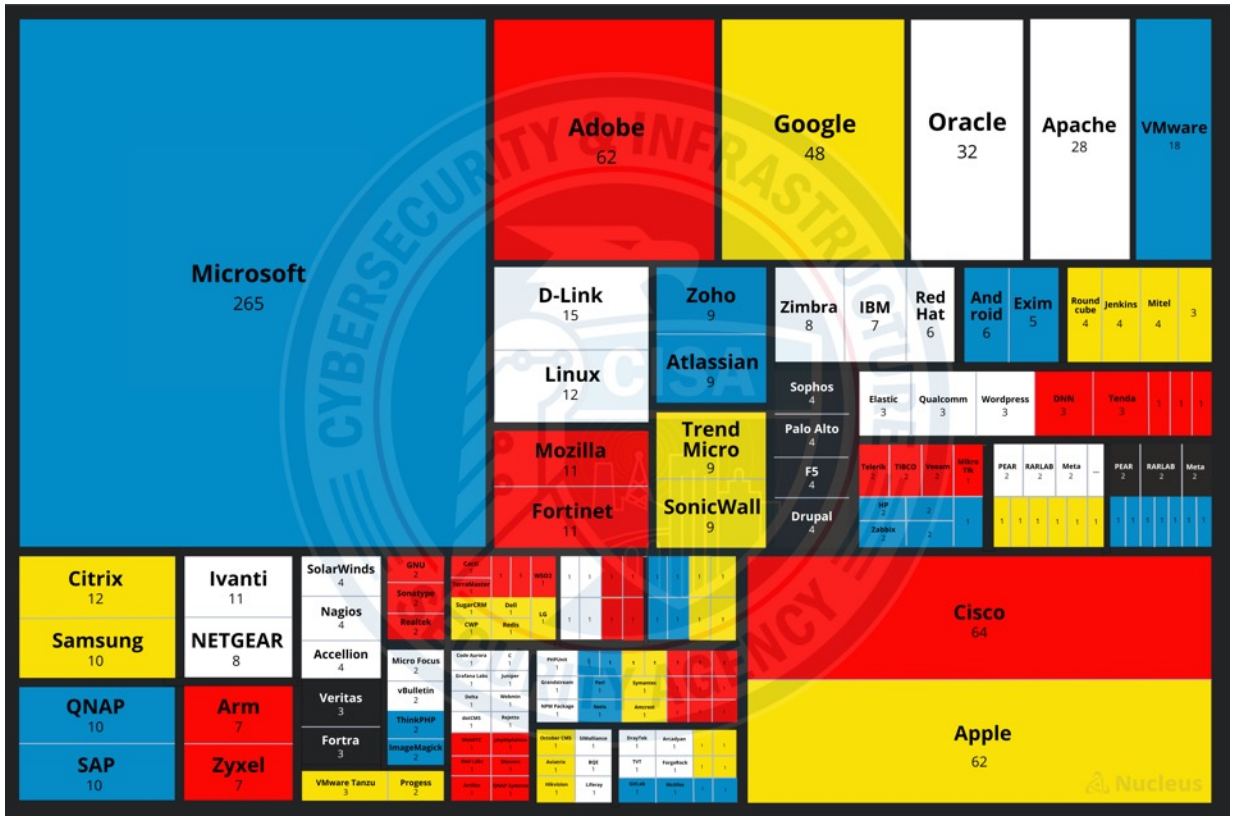
Fix: Patching

"Just as regular maintenance keeps machine gears running smoothly, patching promptly fixes vulnerabilities, and prevents breaches."

Patching Program

1. Establish a Patching Policy
2. Prioritize Patches Based on Risk
3. Test Patches
4. Automate Patch Deployment
5. Schedule Regularly
   - Except for highs
6. Monitor
7. Leverage Threat
8. Use CISA KEV
   - Known Exploited Vulnerabilities
9. Communicate to the Board

CISA Known Exploited Vulnerabilities Catalog

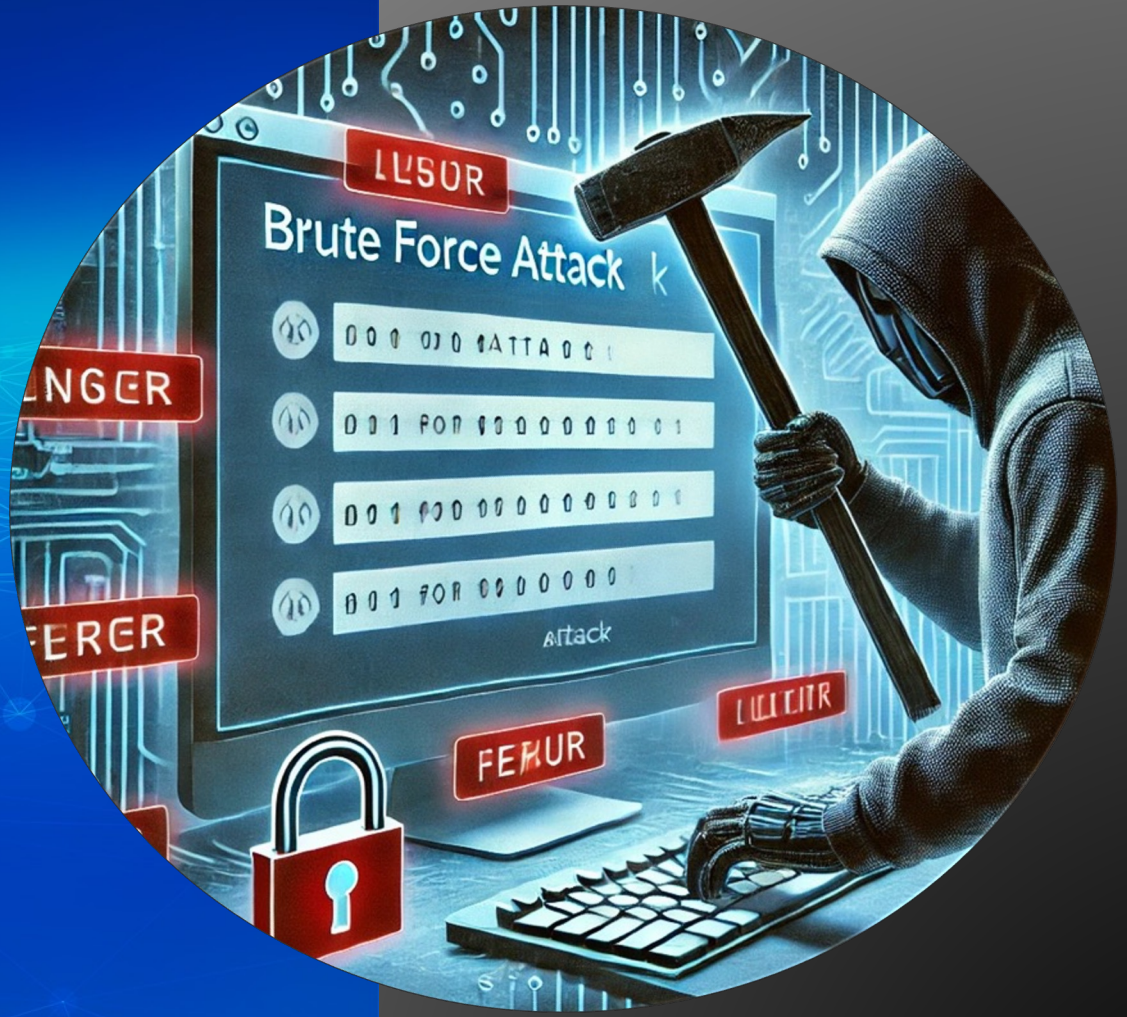


Source: https://nucleussec.com/cisa-kev-art/


PUMPKIN PATCH
CYBER PATCH
CYBER TATCH

Brute Force

Fix: Threat Intelligence / Incident Response



“Don't let a cyber attack strip the threads of your business – tighten up with cybersecurity solutions & processes.”

Threat Intelligence Overview

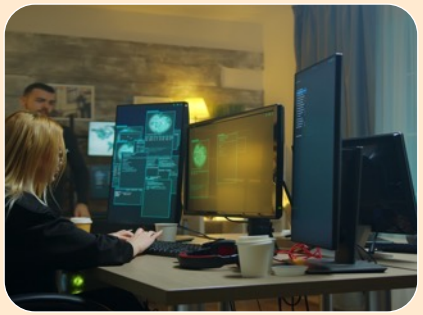
- Understand Attacker Tactics
- Know Your Assets
- Identify Indicators of Compromise (IoCs)
- Enhance Incident Response
- Update Security Policies

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." – Sun Tzu, The Art of War

Threat Landscape – the actors

Nation state

- Strategic
- Political
- Espionage



Cybercrime Groups

- Ransomware
- Organized
- Cyber Mafia

Hacktivist

- Political
- Social

Competitors

- Espionage
- Int. Property

Disgruntled Employee

- Frustration
- Espionage
- Self Serving
- Insider Threat

Broken Windows Approach – Identifying Critical Systems

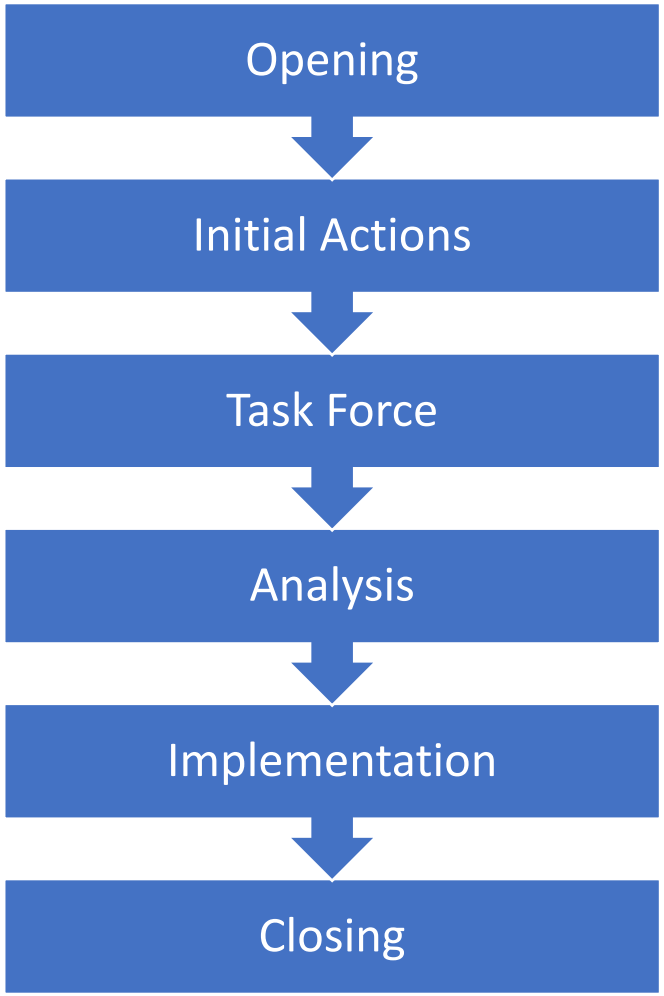
Questions

- Where is my most important data?
- Where are most of my incidents happening?
- Where am I most vulnerable?
- What is (are) the worst possible thing(s) that could happen?
- Can I detect where I am most vulnerable?
- Can contain where I am most vulnerable?
- Can I see the insider threat?

Answers

- Identify your “broken windows”
- Establish network visibility
- Segment to protect critical assets, create security zones
- Layered defensive strategy
- People Process, Technology
- Get control of your elevated privileges, if you can
- Train and Educate managers and HR about high-risk employees with elevated privileges

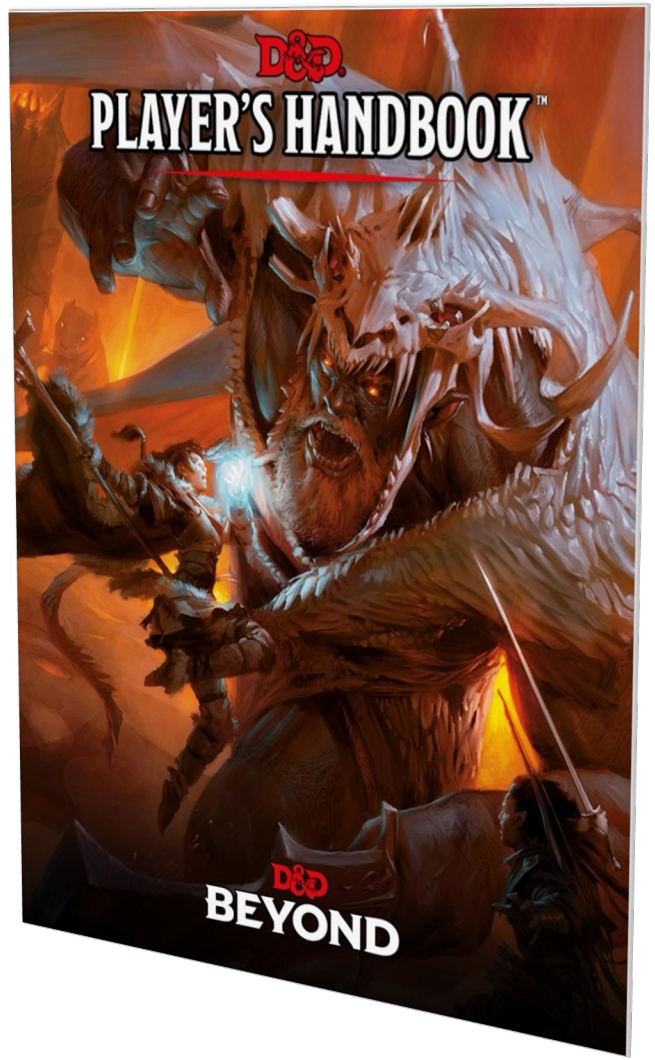
Incident Handling – Another Process



- Incident handling covers reactive activities for remediating and mitigating incidents
- Process of analyzing, evaluating and resolving security events that occur in a deployed within an organization
- The direct or indirect compromise of confidentiality, integrity and / or availability (CIA) of the organization.
- A single event or a series of unwanted or unexpected events that compromise operations and threaten CIA
- Consider for each case handled, a task force is set up for tracking and management.
- **Like on an airplane, football team, test regularly**

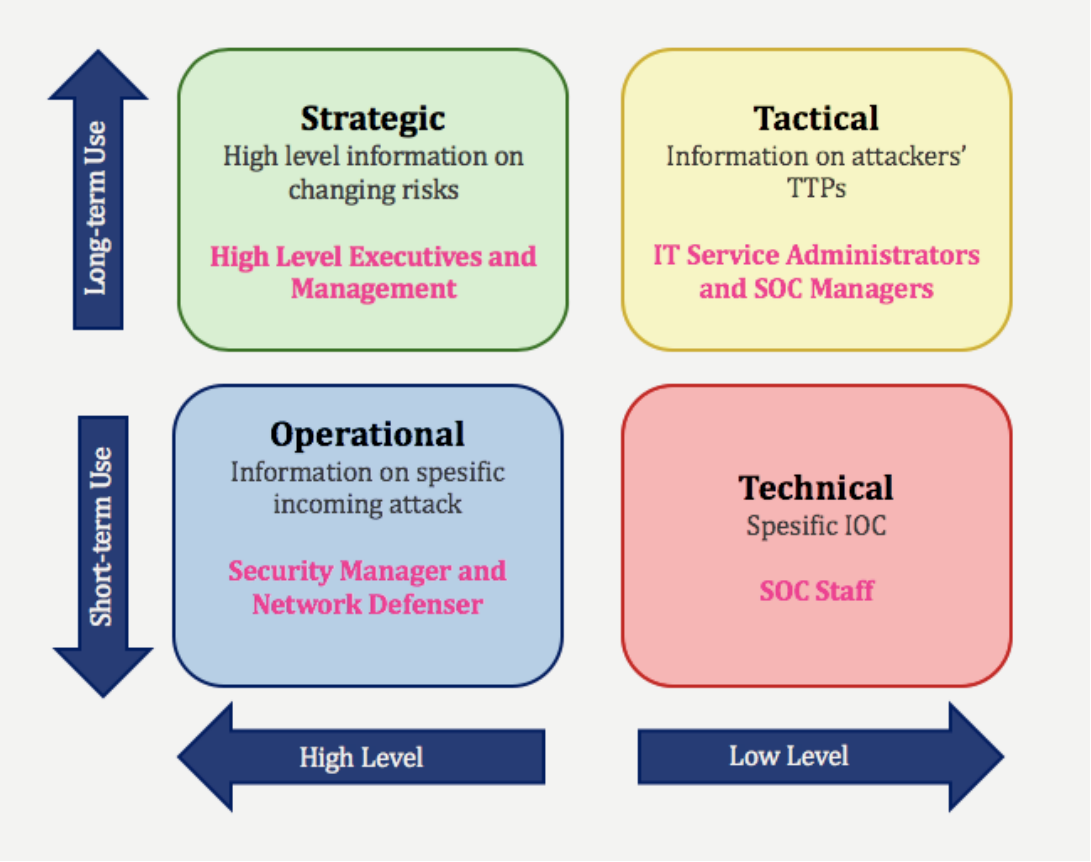
Testing – Successful TTXs

1. Make sure your tabletop exercise is your tabletop exercise.
2. Explore a scenario beyond just the technical aspects.
3. Get top-level management on board.
4. The facilitator is key.
5. You're testing people, not technology.
6. Build your scenarios based on active threat intelligence.
7. Participants need to get into character.
8. Don't let the party get too big.
9. Give your exercise the amount of time it deserves.
10. Create a safe space for experimentation—and failure



Threat Intelligence Program

- Define requirements and objectives
- Identify relevant threat data sources
- Implement tools for data collection and processing
- Establish analysis procedures and workflows
- Integrate threat intelligence into security controls
- Continuously update and refine the program




Why doesn’t Superman help us fight cybercrime?
He’s afraid of Krypto-currency

Malicious Email / Phishing

Security Awareness & Assessments

KnowBe4
Human error. Conquered.

"In manufacturing, a single faulty gear can halt production; in cybersecurity, a single click can halt your organization."

Social Engineering

"Any act that influences a person to take an action that may or may not be in their best interest."

Biggest Initial Breach Root Causes for Most Companies

- Social engineering was the #1 root cause of hacking and malware
- Verizon Data Breach Investigation Report – 68% of all attacks are human related
- <30 seconds from phish to credential loss

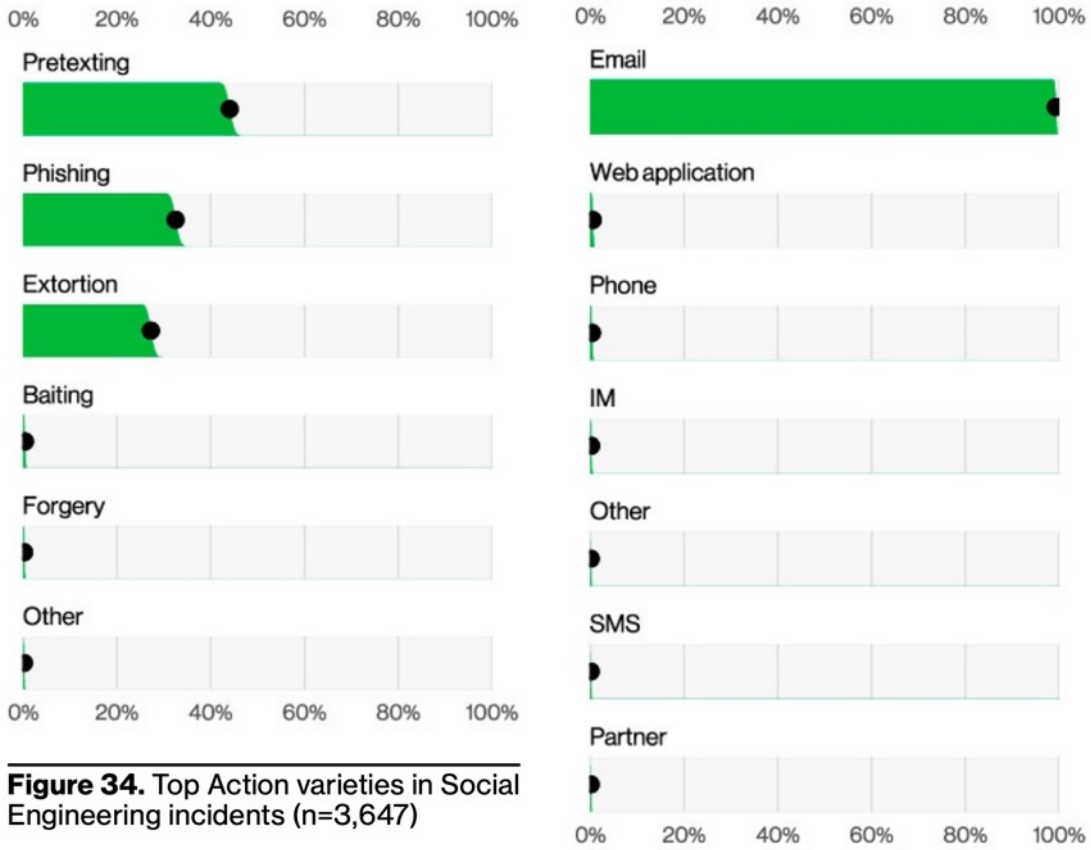


Figure 34. Top Action varieties in Social Engineering incidents (n=3,647)

Social engineering is responsible for majority of all malicious data breaches

Phishing

Anyone with an

email address,

has a key to the front door.

They can open the front door

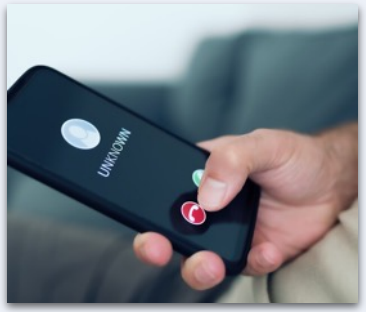
and let in the cyber criminals

into the organization.

*ishing Attack Vectors (Social Engineering)

Spear Phishing

SMSishing



Vishing

Whaling

Snowshoeing

Tishing

Wishing

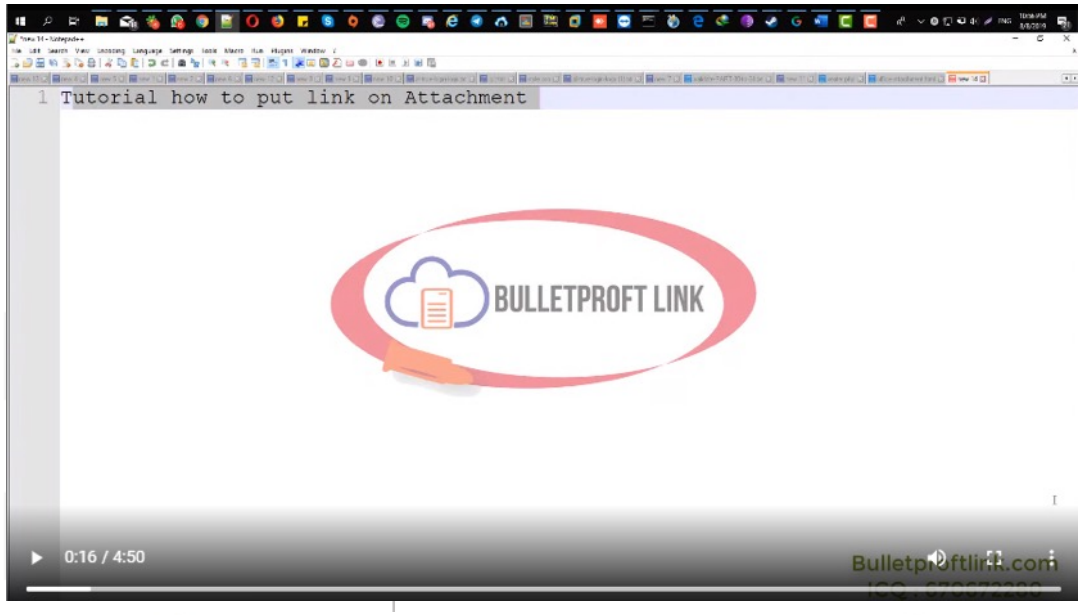
Pharming

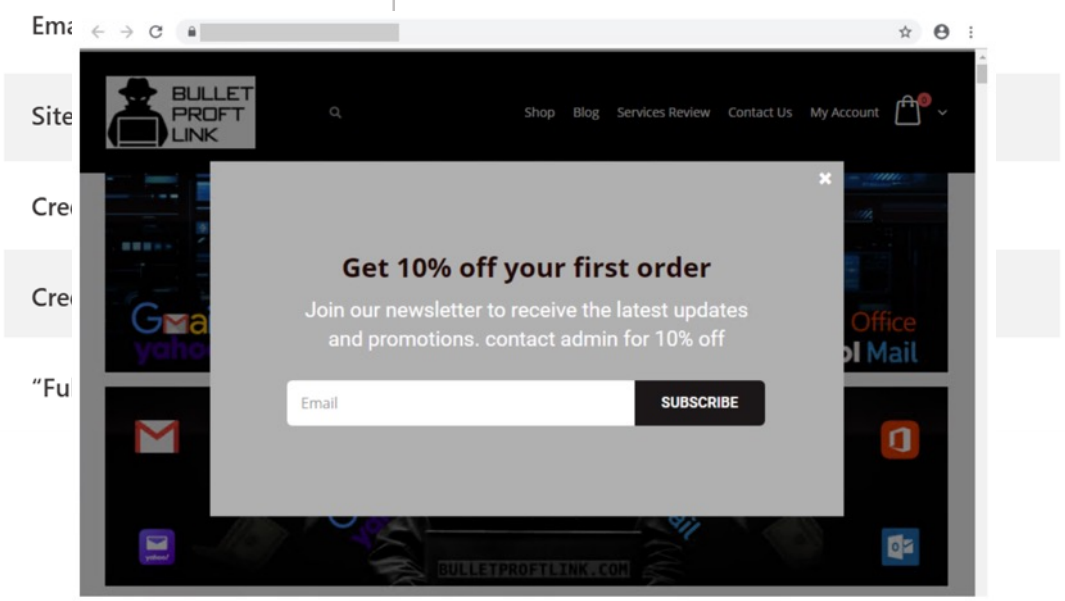
Watering Hole

QR Code Phishing

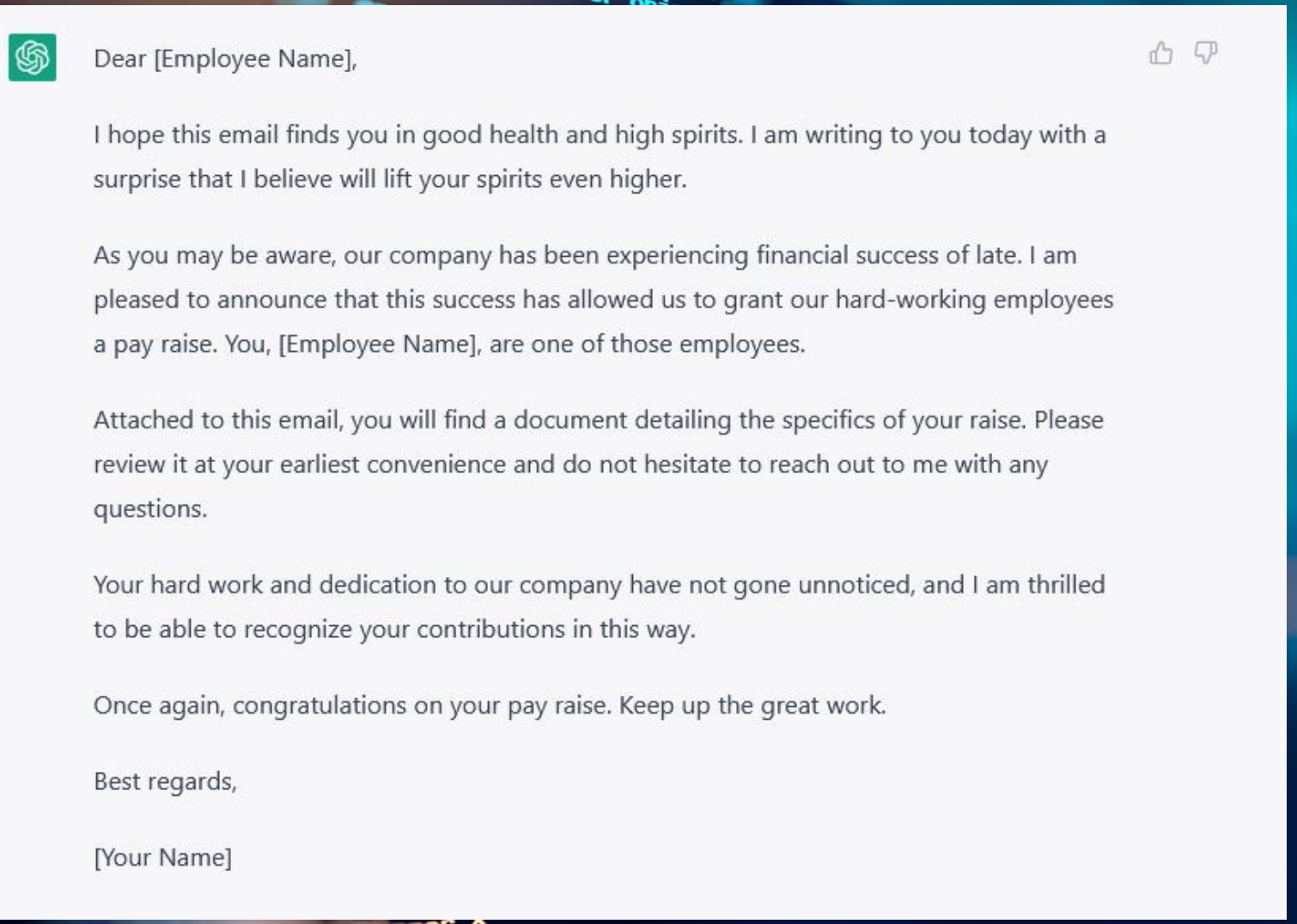
Phishing as a Service

- Allows non-technical people to launch their own attacks
- Multiple tiers of service
- Phishing kits that contain the tools needed to set up campaign
- Fully managed services for all types of phishing
- Tutorials or training are often included, or available as well





The Cybercriminals are using **AI** to **level-up** their **attacks**.



Are You Being Manipulated? – Emotional Lures

Greed

Urgency

Fear

Helpful

Self-Interest

Curiosity

Vishing / Deepfake Voice Call

SMS to 27 employees at an organization

1 clicked the link

Entered MFA credentials

Called the victim and posed an IT member using deepfake audio

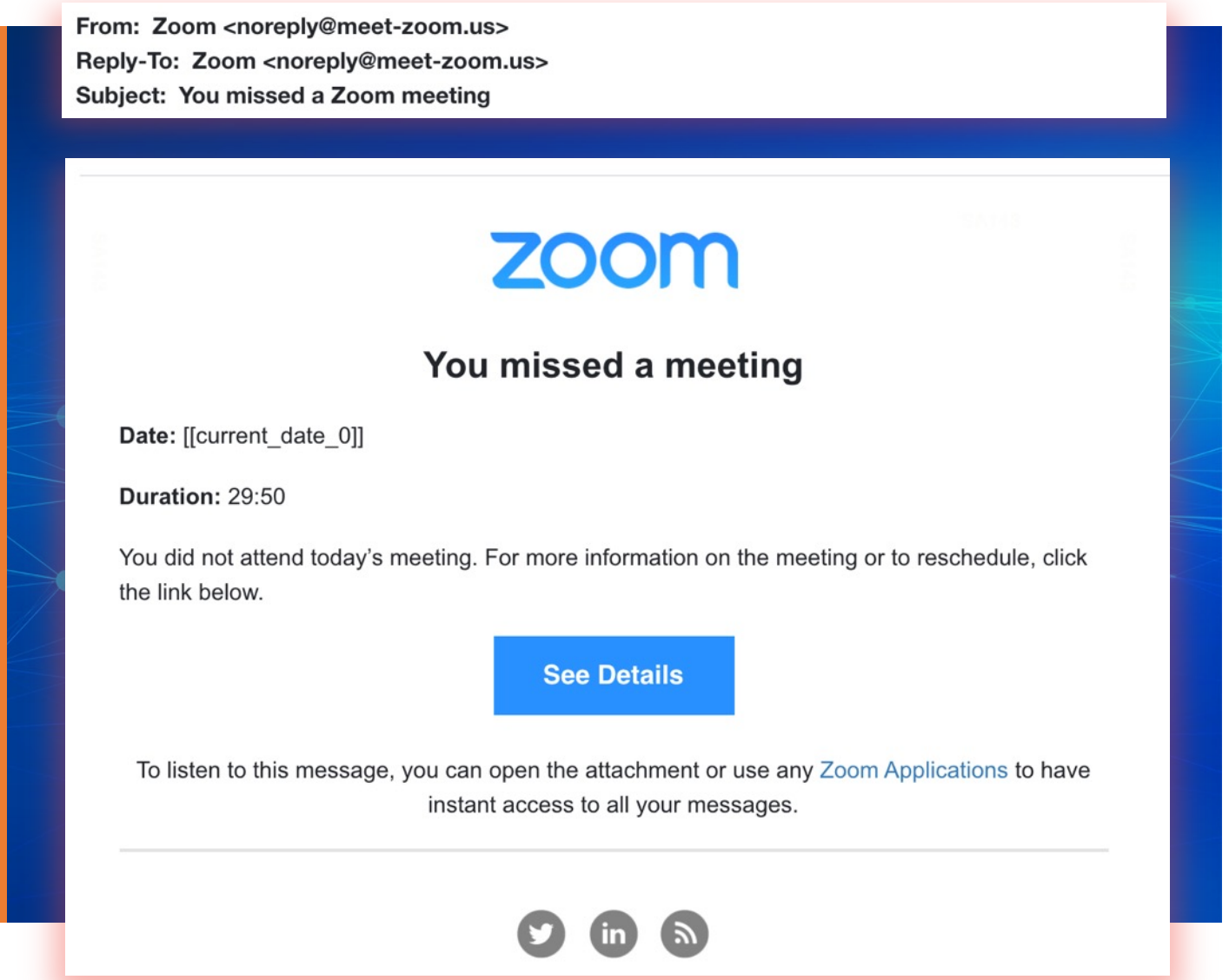
Socially engineered to give up code

Access to Authenticator, and other apps

Social Engineering – CEO Fraud


NBR

Phishing Example



Stages of Post Phishing / Social Engineering Attack

Shock

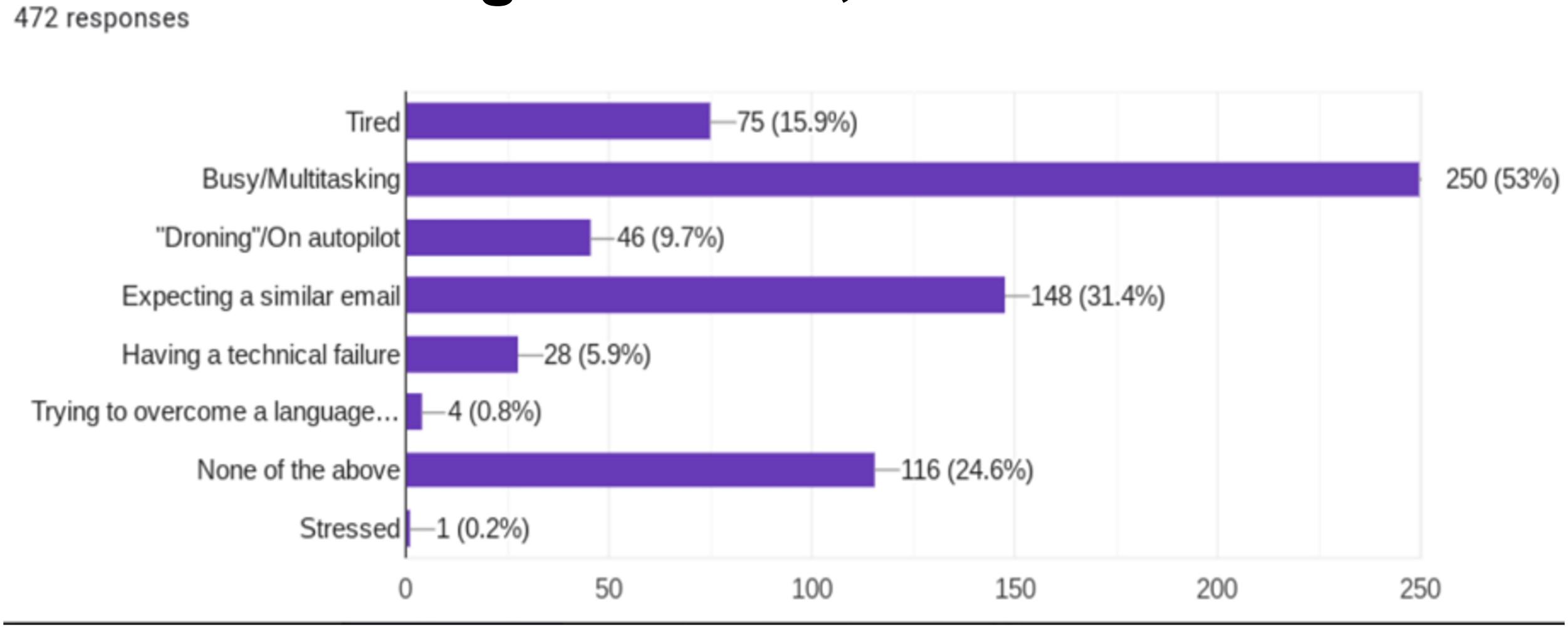
Denial

Anger

Acceptance

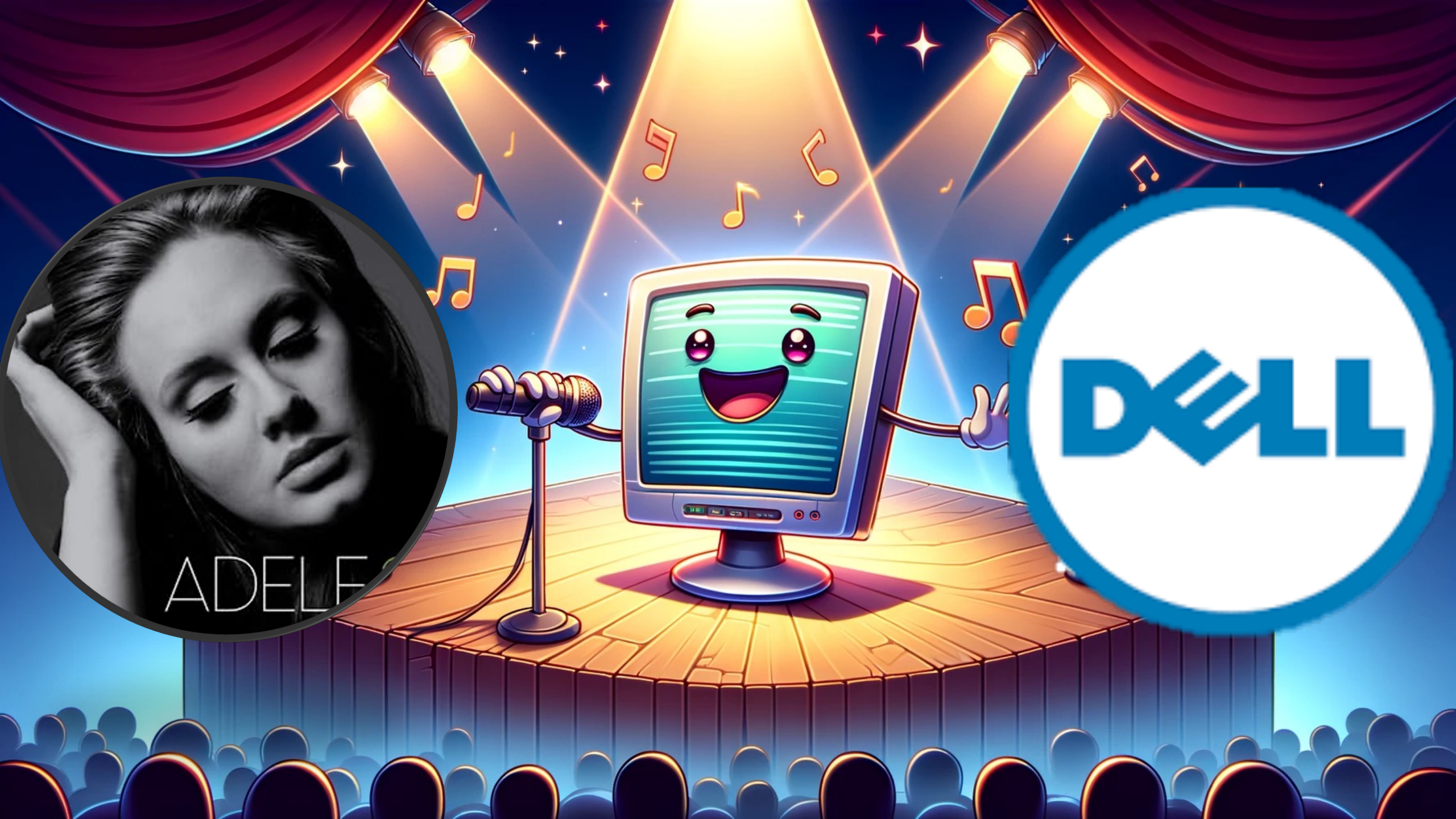
It’s a Teaching Moment

When Viewing the Phish, I was…



Who’s At Risk?

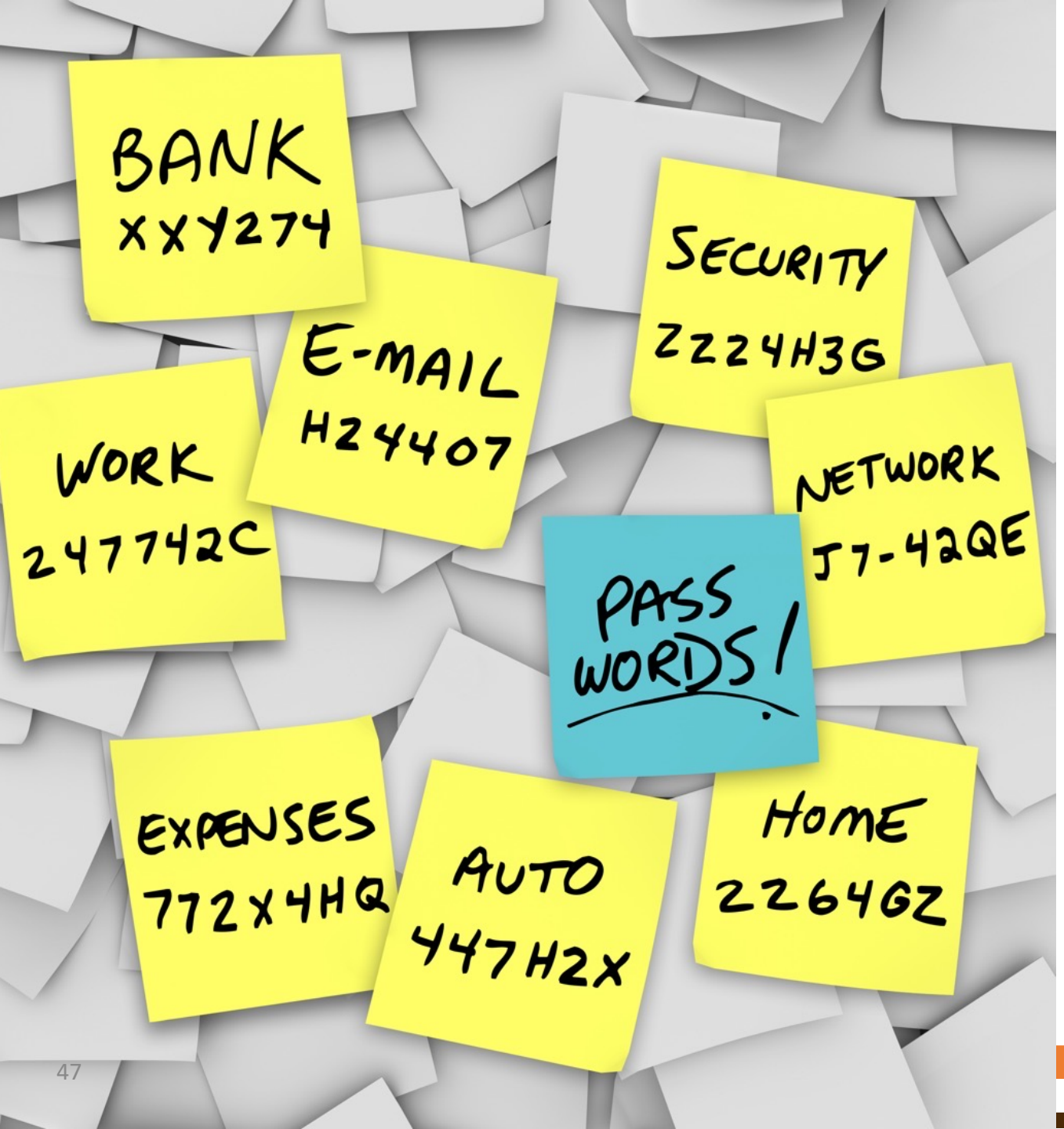
- New, seasonal or temporary employees
- Senior people (managers, directors, privileged users)
- Maintenance staff (cleaners, security guards, vendors)
- People who are active or chatty on social media.
- HR departments
- **Everyone is at risk**


ADELE
DELL

Credential Stuffing

Fix: Strong Passwords

"In the world of manufacturing, strong gears and strong passwords are both essential for keeping things running."



Password Attacks

Akamai: We Saw 61 Billion Credential Stuffing Attacks in 18 Months

PCWorld

News

Time to update your password: 26 billion personal records leaked

The data set clocks in at a massive 12TB.

Credential Stuffing / Phishing

Credential stuffing:

- Uses lists of usernames, email addresses with passwords
- Large-scale automated login requests.

Credential Phishing:

- Using phishing, vishing SMSishing attacks to get users to give up their credentials

Multi Factor Authentication (1 Factor, 2 Factor, 3 Factor)

SMS (Restricted by US Government)

- It's okay – not the best
- Unfortunately, this is commonly used

Application (Phishable with MitM Attacks)

- Code Generated in App
- Make sure you can back them up

Hardware (FIDO Approved)

- Uses a hardware token, like a Yubikey or your smartphone
- Can be inconvenient when forgotten or damaged

Tooth Factor Authentication

Password Use Recommendations - DiNGS

MFA	If possible, use MFA
Unique Passwords	Unique & Complex passwords
Password Manager	It creates DiNGS
Create your own?	At least 12 characters, complex
Better	16+ character / passphrase

Different, Non-Guessable, Strong Passwords

Most Secure Woman?

MFA

Emma Faye

Multifactor Authentication

Defending

”Cybersecurity is the lubricant that keeps your manufacturing operations from seizing up under pressure.

Incident Response


Opening


Initial Actions


Task Force


Analysis


Implementation

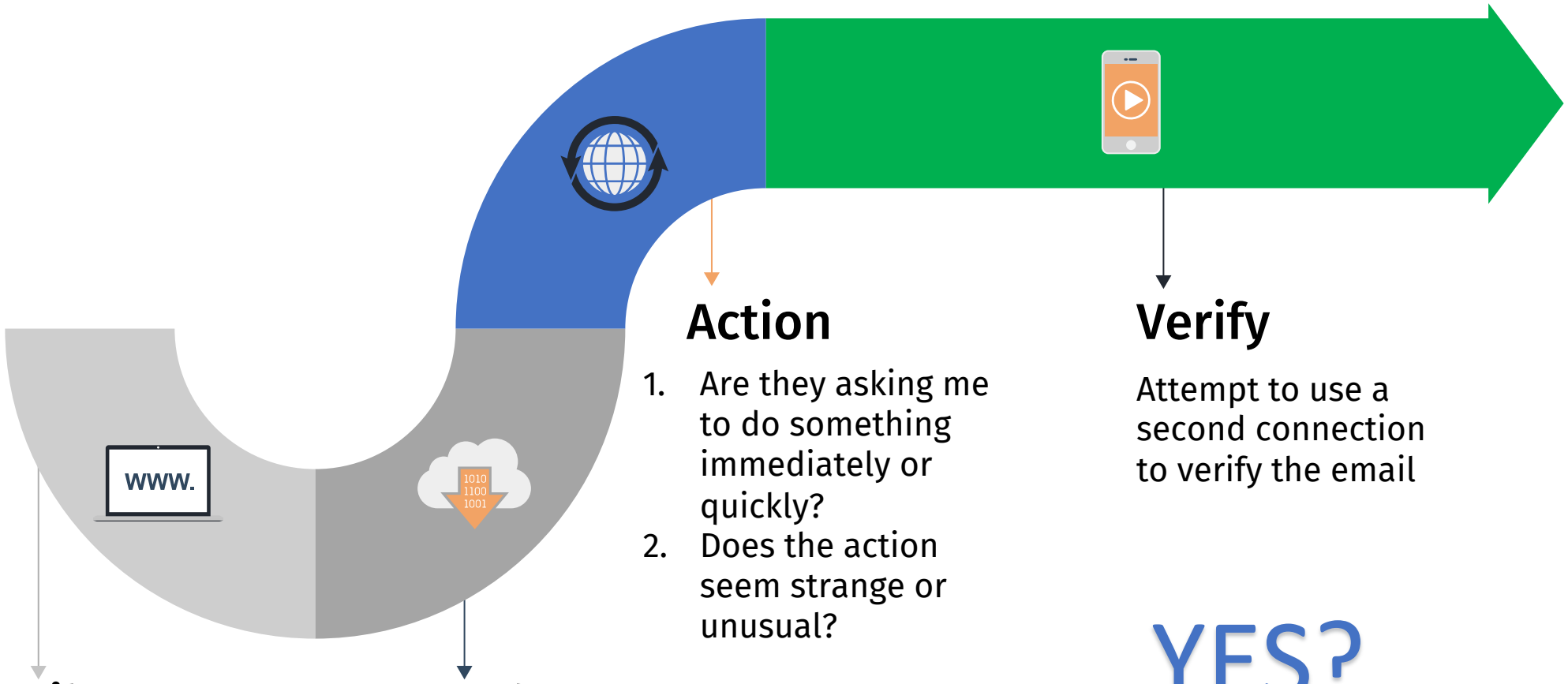

Closing

- Don’t overrate an incident, stick to the facts
- Communicate, Communicate, Communicate
- Analyze your environment; Know your strengths and weaknesses
- Ensure you understand the threat’s capabilities, intent and vectors
- Focus your response on your “broken windows”
- Ensure you are achieving success and not reinforcing failure in your Incident Response processes
- Keep an offline copy of IR Playbook

Social Engineering Defense in Depth

Mitigate	• Aggressively Mitigate Social Engineering • People, Processes, Technology
Patch	• Patch Exploited Software & Firmware • Monitor the CISA KEV Catalog (Known Exploited Vulnerabilities)
MFA	• Use MFA Wherever Possible • Non-phishable MFA too, Avoid SMS and verify all requests that you didn't initiate
SPOT	• Learn how to Spot Rogue URLs • No longer – don't click on links, or check your links, make sure they know how
DiNGS	• Remember to use DiNG style of passwords • Different, Non-Guessable, Strong

3 Questions to Ask Your Email



Email

Is the email unexpected?

Sender

Is this person a stranger? #StrangerDanger

Action

1. Are they asking me to do something immediately or quickly?
2. Does the action seem strange or unusual?

Verify

Attempt to use a second connection to verify the email

YES?

Mindfulness and Your Email

Awareness

Recognition

Focus

Intentionality

Responsiveness

Zero Trust Mindset

- Not trusting anything by default
- Verifying everything

- Applied to humans it calls for:
  - Politely Paranoid
  - Be skeptical
  - Constant verification

- Mindfulness practices encourage to:
  - pause before reacting
  - engage intentionally and thoughtfully.

Security culture is defined as the ideas, customs, and social behaviors that impact the security of your organization.

SAFETY FIRST

DAYS SINCE
LAST CYBER INCIDENT

7 Tips For A Better Security Culture

1. Choose Behaviours

2. Plan for ‘Behaviour Design’ – BJ Fogg

3. Get Leadership Buy In

4. Communicate – Newsletters / Videos

5. Execute

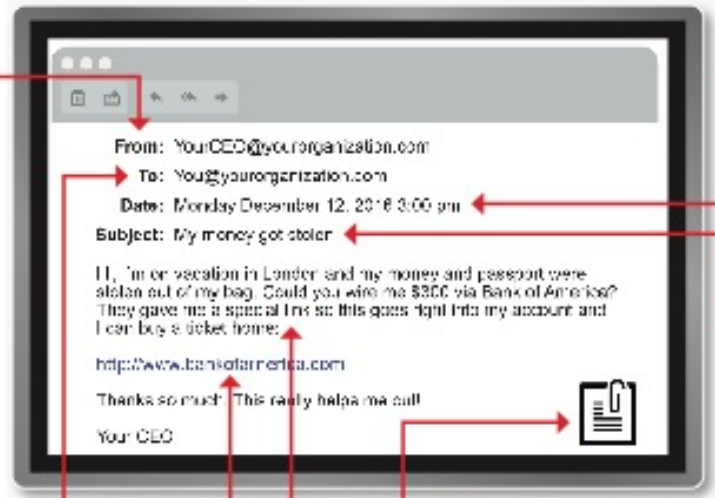
6. Measure Results - Surveys

7. Repeat

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

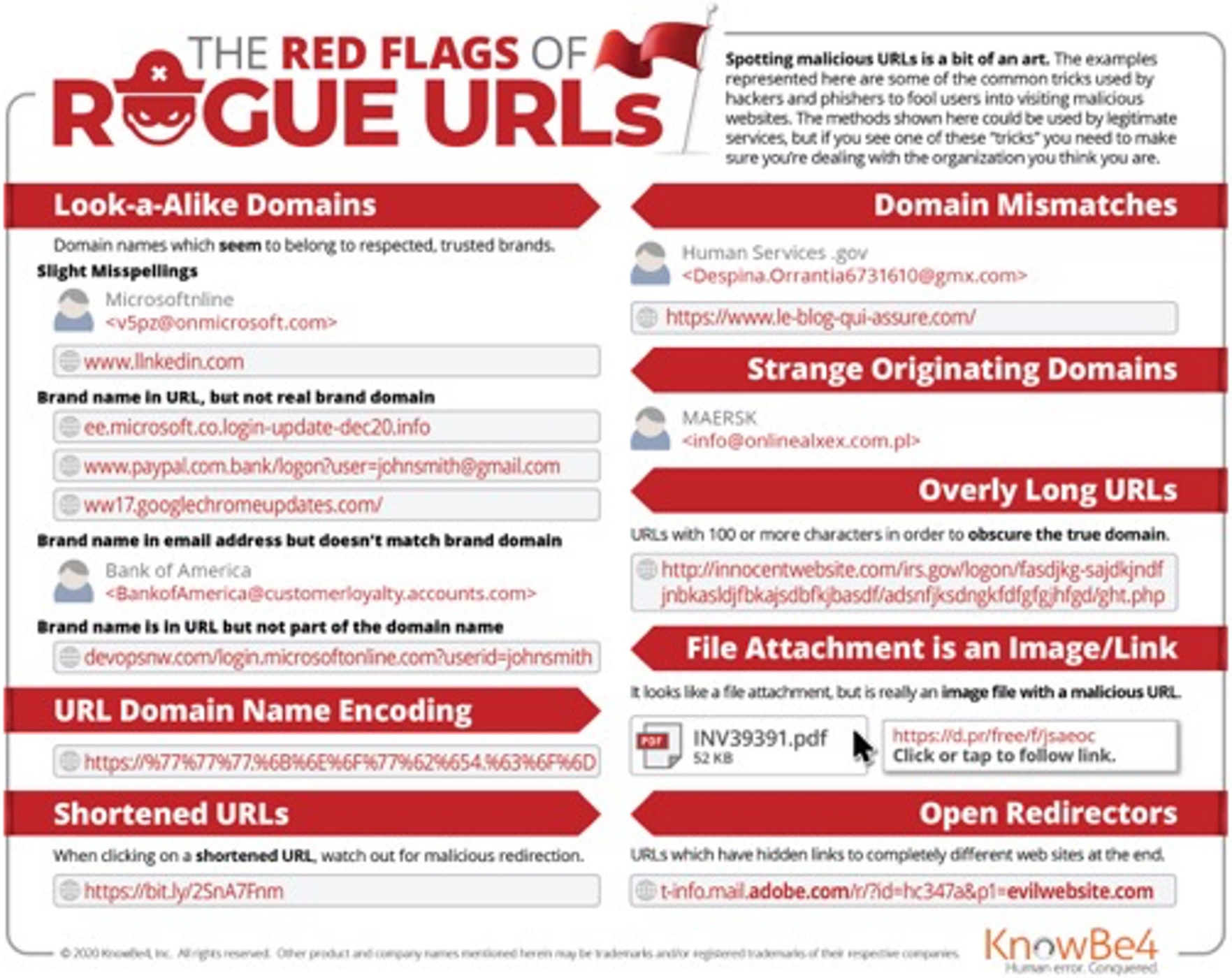
HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.



Rogue URL Tip Sheet


OLD HABITS
CHANGE


HOW DO TREES
GET ONLINE?

Final Thoughts

"From the shop floor to the server room, secure every aspect of your manufacturing with comprehensive cybersecurity."

How To Protect Against These Attacks

Exploited Vulnerabilities

Gotta Patch It!

Compromised Credentials

Don’t Reuse Old Passwords

Malicious Email

Use AI / Secure Email Gateways

Phishing

Security Awareness Training / Culture

Brute Force Attack

Be aware of Supply Chain Attacks

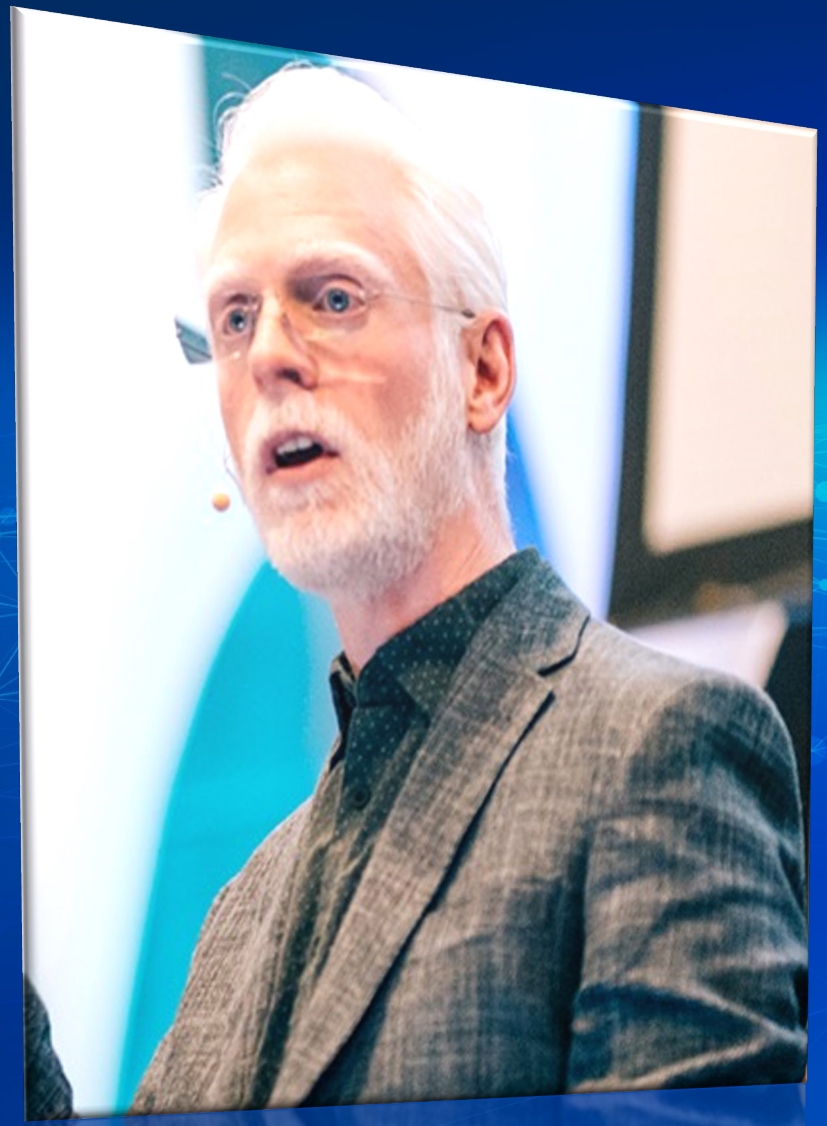
Humans are the
number one attack vector and
a critical layer of of your security program.

Building a

HUMAN FIREWALL

is about the intersection between ***Awareness***, ***Intention***, and ***Behavior***.

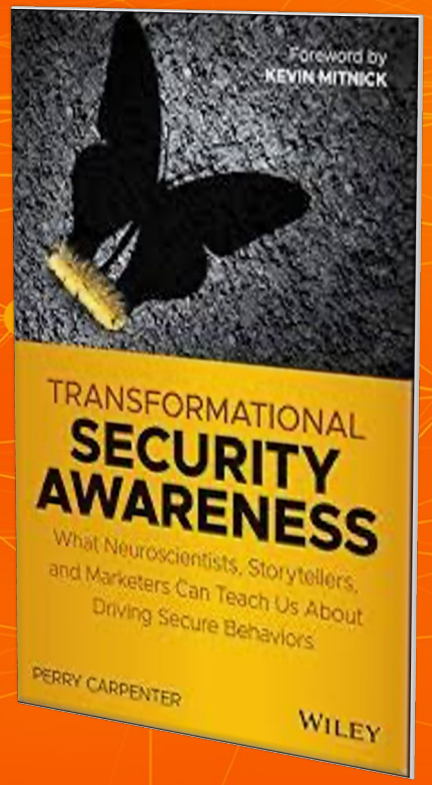
What it's like for the IT Team

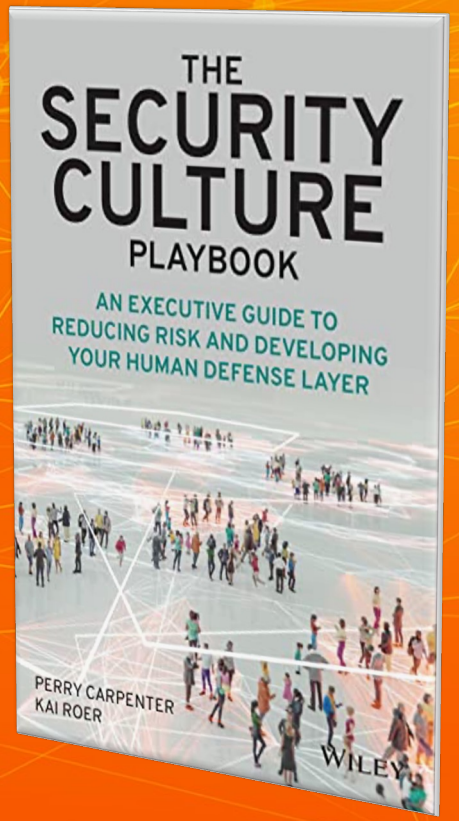


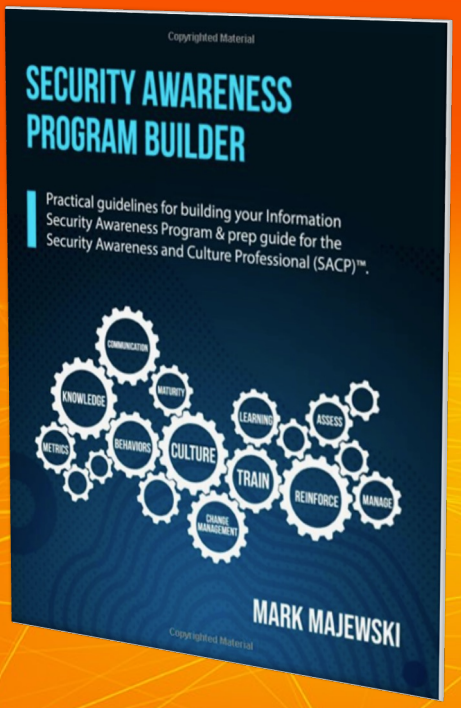
This goes way beyond awareness or coercing secure behaviors. It's about making workers value security …where they proactively participate in taking steps that reduce risk.

-Perry Carpenter

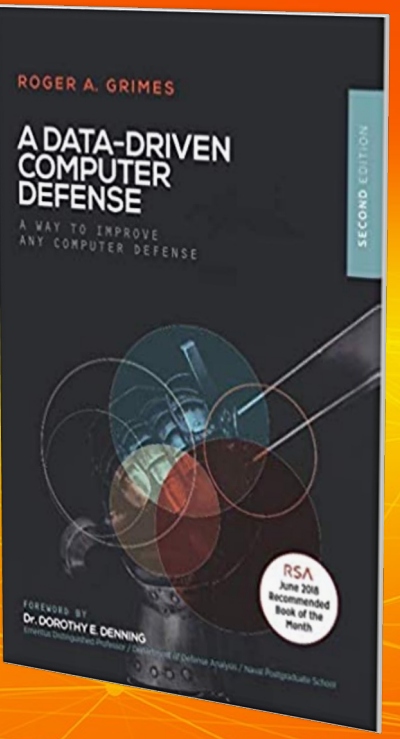
Resources

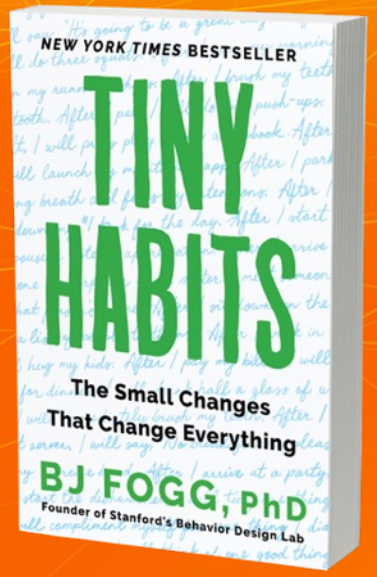

Foreword by
KEVIN MITNICK
TRANSFORMATIONAL
SECURITY
AWARENESS
What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors
PERRY CARPENTER
WILEY

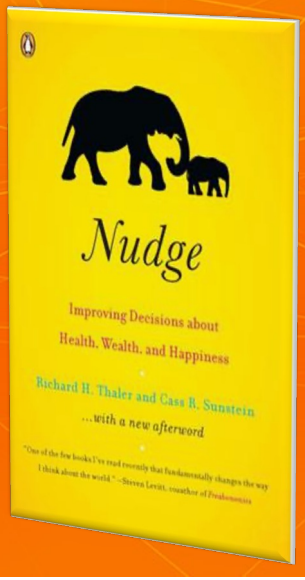

THE
SECURITY
CULTURE
PLAYBOOK
AN EXECUTIVE GUIDE TO REDUCING RISK AND DEVELOPING YOUR HUMAN DEFENSE LAYER
PERRY CARPENTER
KAI ROER
WILEY


Copyrighted Material
SECURITY AWARENESS
PROGRAM BUILDER
Practical guidelines for building your Information Security Awareness Program & prep guide for the Security Awareness and Culture Professional (SACP)™.
MARK MAJEWSKI


CYBERSECURITY
ABCs
Delivering awareness, behaviours and culture change
Jessica Barker, Adrian Davis, Bruce Hallas and Ciarán Mc Mahon


ROGER A. GRIMES
A DATA-DRIVEN COMPUTER DEFENSE
A WAY TO IMPROVE ANY COMPUTER DEFENSE
SECOND EDITION
RSA
June 2018 Recommended Book of the Month
FOREWORD BY
Dr. DOROTHY E. DENNING


NEW YORK TIMES BESTSELLER
TINY
HABITS
The Small Changes That Change Everything
BJ FOGG, PhD
Founder of Stanford's Behavior Design Lab

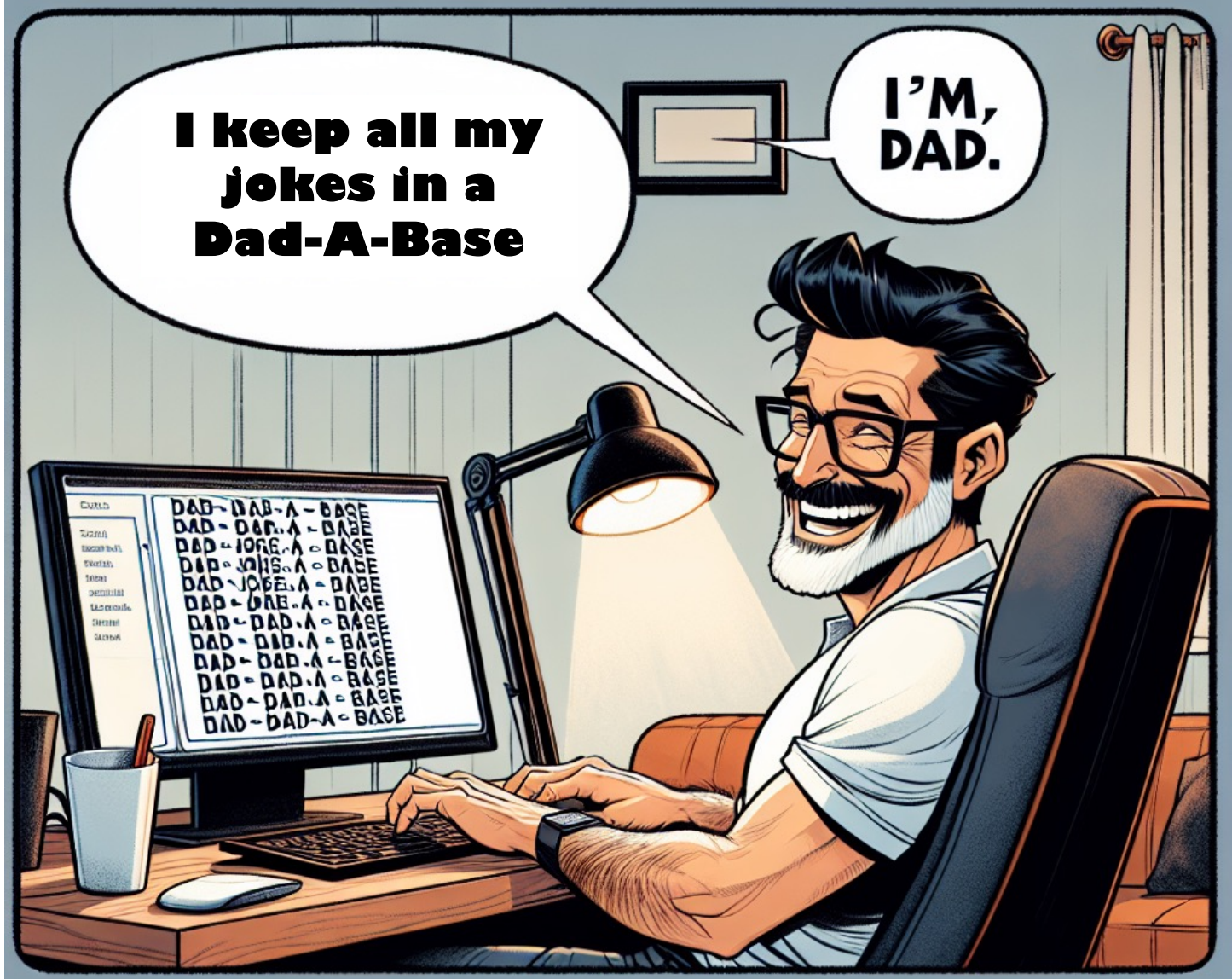

Nudge
Improving Decisions about Health, Wealth, and Happiness
Richard H. Thaler and Cass R. Sunstein
...with a new afterword

securitymasterminds.buzzsprout.com

SECURITY MASTERMINDS PODCAST

The podcast that brings you the very best in all things, cybersecurity, taking an in-depth look at the most pressing issues and trends across the industry.

Yes… I have a way of keeping track of my Dad Jokes



James R. McQuiggan, CISSP

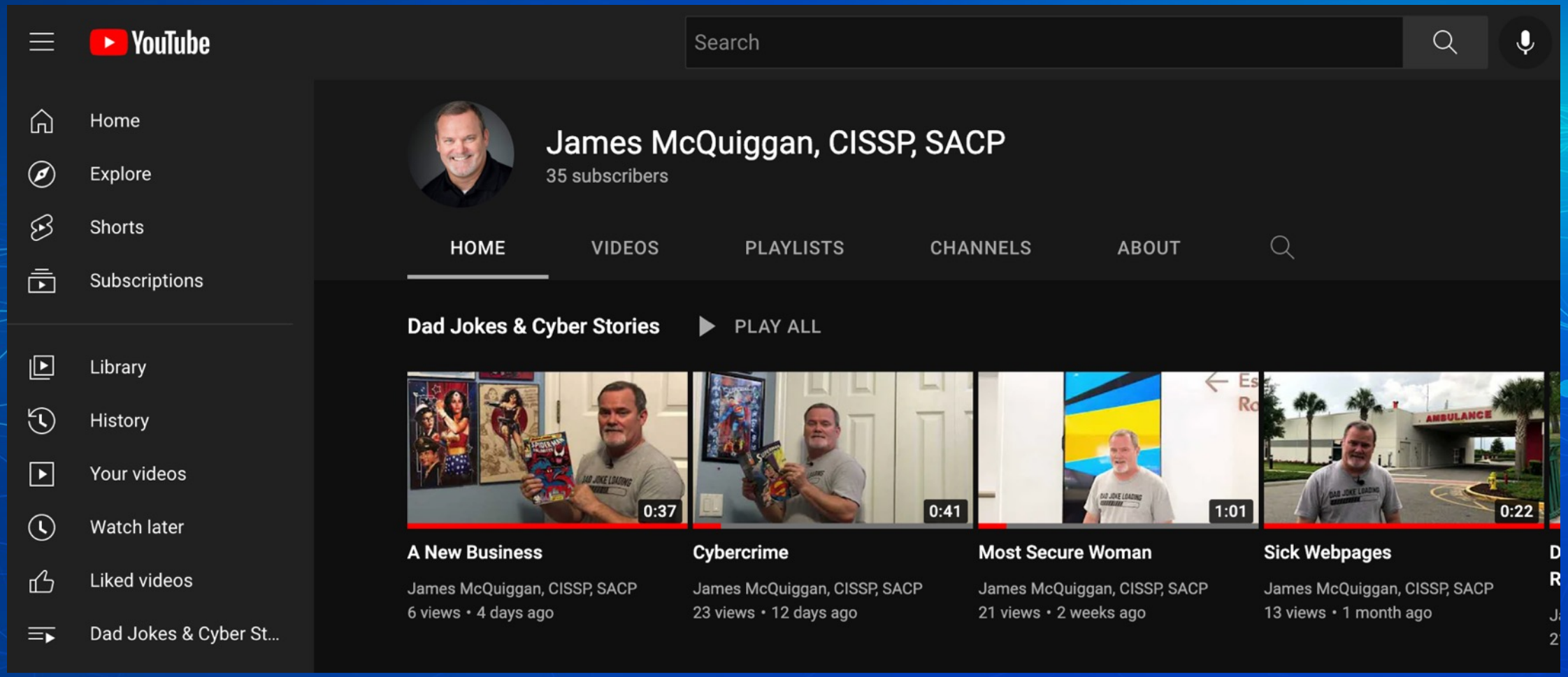
jmcquiggan@knowbe4.com

LinkedIn: jmcquiggan

X: @james_mcquiggan

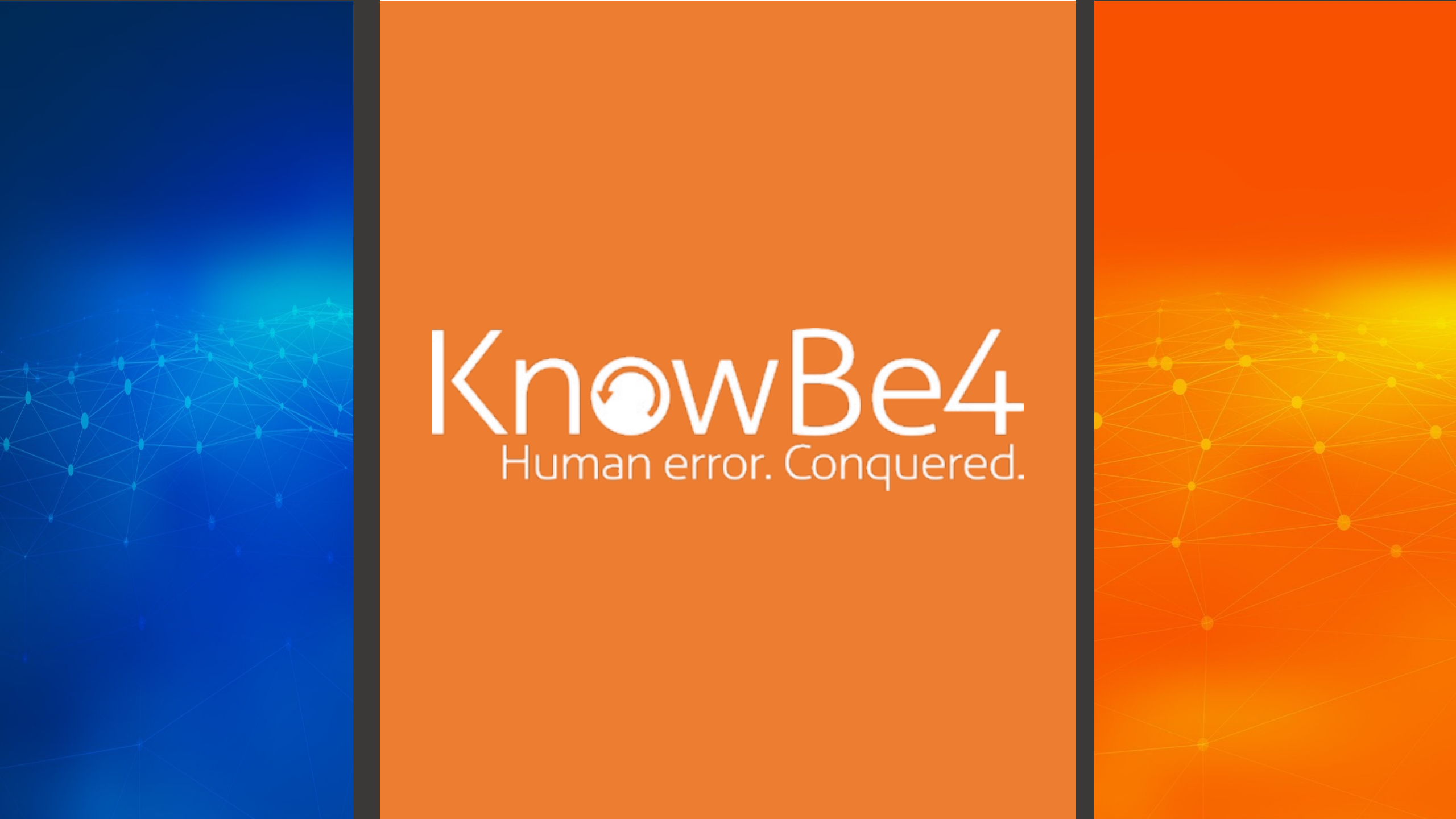
blog.knowbe4.com

KnowBe4
Human error. Conquered.



YouTube: James McQuiggan and Dad Jokes

https://www.youtube.com/@JamesMcQuigganCISSP


KnowBe4
Human error. Conquered.

KnowBe4
Human error. Conquered.

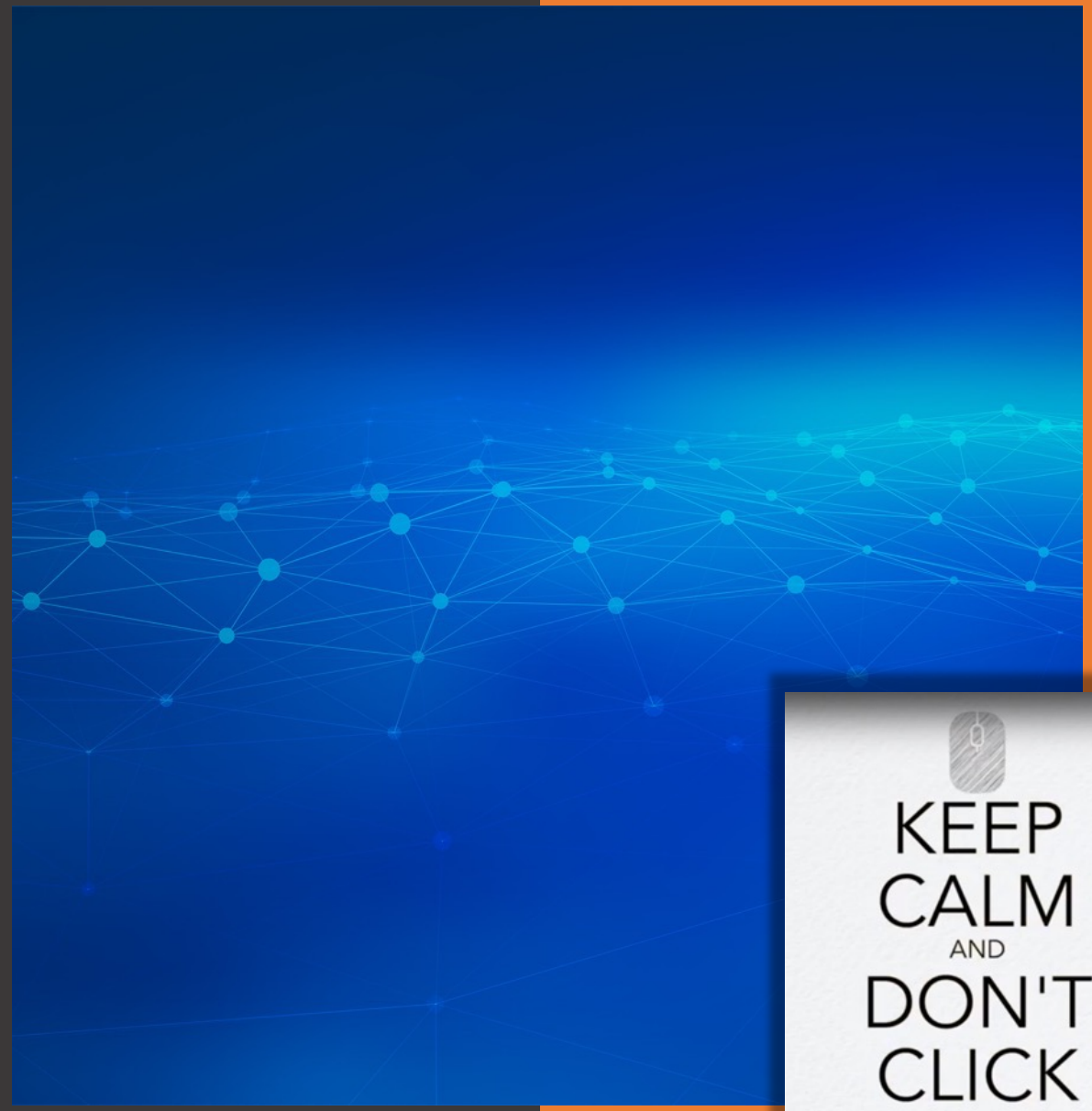
For more information visit
blog.knowbe4.com

James R. McQuiggan, CISSP

jmcquiggan@knowbe4.com

Twitter: @james_mcquiggan

LinkedIn: jmcquiggan



Resources

- **Contact Info**
  - LinkedIn: https://www.linkedin.com/in/jmcquiggan/
  - Twitter: https://twitter.com/James_McQuiggan
  - Email: jmcquiggan@knowbe4.com
- **KnowBe4**
  - Blog – https://blog.knowbe4.com
  - Social Engineering Red Flags PDF - https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf
  - Rogue URLs PDF - https://www.knowbe4.com/hubfs/Red%20Flags%20of%20Rogue%20URLs%20(3).pdf
  - Rogue URL webinar: https://blog.knowbe4.com/combatting-rogue-url-tricks-how-you-can-quickly-identify-and-investigate-the-latest-phishing-attacks
  - Phishing Benchmark Report - https://info.knowbe4.com/phishing-by-industry-benchmarking-report
  - KnowBe4 Home Course Training (password: homecourse) https://www.knowbe4.com/homecourse
  - Ransomware Hostage Rescue Manual: https://www.knowbe4.com/ransomware
  - KnowBe4 Compliance Manager - kcmgrc.knowbe4.com

Discussions With C-Suite/BoD

For the C-Suite:

- Support a Culture of Cyber Hygiene
- Allocate Adequate Resources
- Understand the Business Impact
- Champion Risk-Based Decision Making

For Boards of Directors:

- Inquire About Patch Management Practices
- Understand Regulatory Requirements
- Evaluate Cybersecurity Posture
- Support Continuous Improvement

Roleplay – Tabletop Exercise (TTX)

Backdoors & Breaches

YouTube: https://www.youtube.com/watch?v=vZLNdZLHKz4 (it's 76 minutes)
Discord Channel: https://discord.gg/bnb
Order your own decks: https://spearphish-general-store.myshopify.com/

Disclaimer: KnowBe4 does not endorse Backdoors & Breaches and James receives no compensation from BHIS for supporting the program. He just finds it really cool and a great way to work through Incident Response Scenarios!

Source: https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/