PAYROLL SECURITY IN THE AGE OF AI

J.D. Mulliken

AGENDA

INTRODUCTION

REGULATORY LANDSCAPE

THREAT LANDSCAPE

CYBERSECURITY & YOUR ORGANIZATION

BUILDING SECURITY CULTURE

NEXT STEPS

Q&A

What are the top 3 security risks to our industry today?

REGULATORY LANDSCAPE

FTC Safeguards Rule

Organizations must adhere to several key requirements under the "Standards for Safeguarding Customer Information".

- Risk Assessment: Conduct regular assessments to identify and mitigate risks to customer data.
- Safeguard Implementation: Implement administrative, technical, and physical safeguards, including access controls, encryption, and monitoring.
- Employee Training: Provide training on data security practices.
- Service Provider Oversight: Ensure that third-party service providers also comply with these standards.
- Incident Response Plan: Develop and maintain an incident response plan to address data breaches effectively.

Source: https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

NACHA Data Security Requirements

This rule supplements previous ACH Security Framework data protection requirements by explicitly requiring Third-Party Senders (TPSs) to protect deposit account information by rendering it unreadable when it is stored electronically.

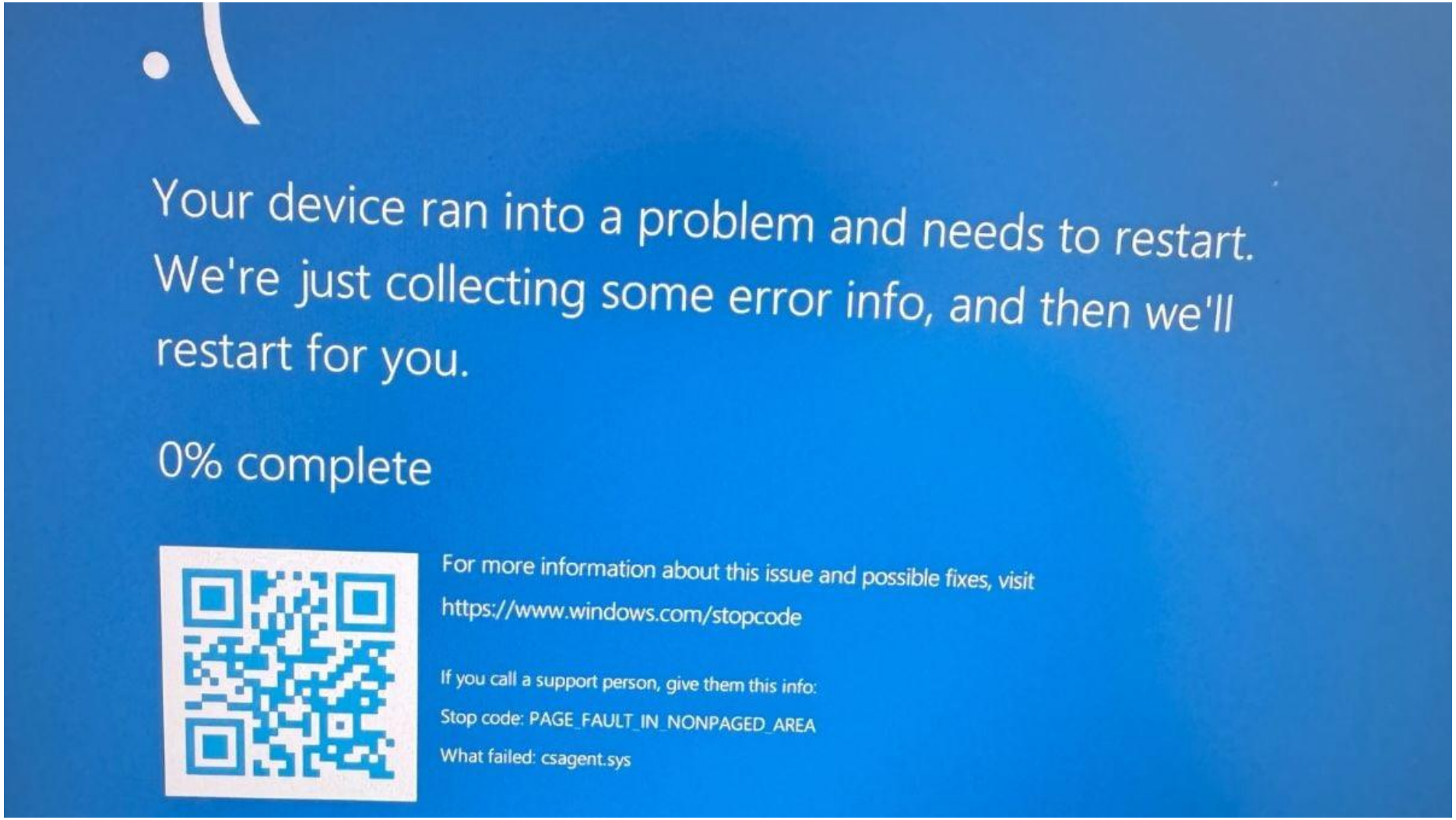
- Encryption: Sensitive data must be encrypted when stored and transmitted.
- Access Controls: Implement strong access controls and multi-factor authentication to protect data.
- Secure Transmission: Use secure protocols (e.g., SFTP) for data transmission and mask sensitive information as needed.
- Annual Audits: Conduct regular audits to ensure compliance with NACHA standards.
- Vendor Management: Ensure third-party vendors comply with NACHA's data security requirements.
- Breach Notification: Promptly notify affected parties and take immediate action in the event of a data breach.

Source: https://www.nacha.org/rules/supplementing-data-security-requirements

THREAT LANDSCAPE

Was July 19th 2024 tech's downfall?

THREAT LANDSCAPE



HUMAN VS. TECH

THIS IS BUT **ONE** EXAMPLE OF MANY…

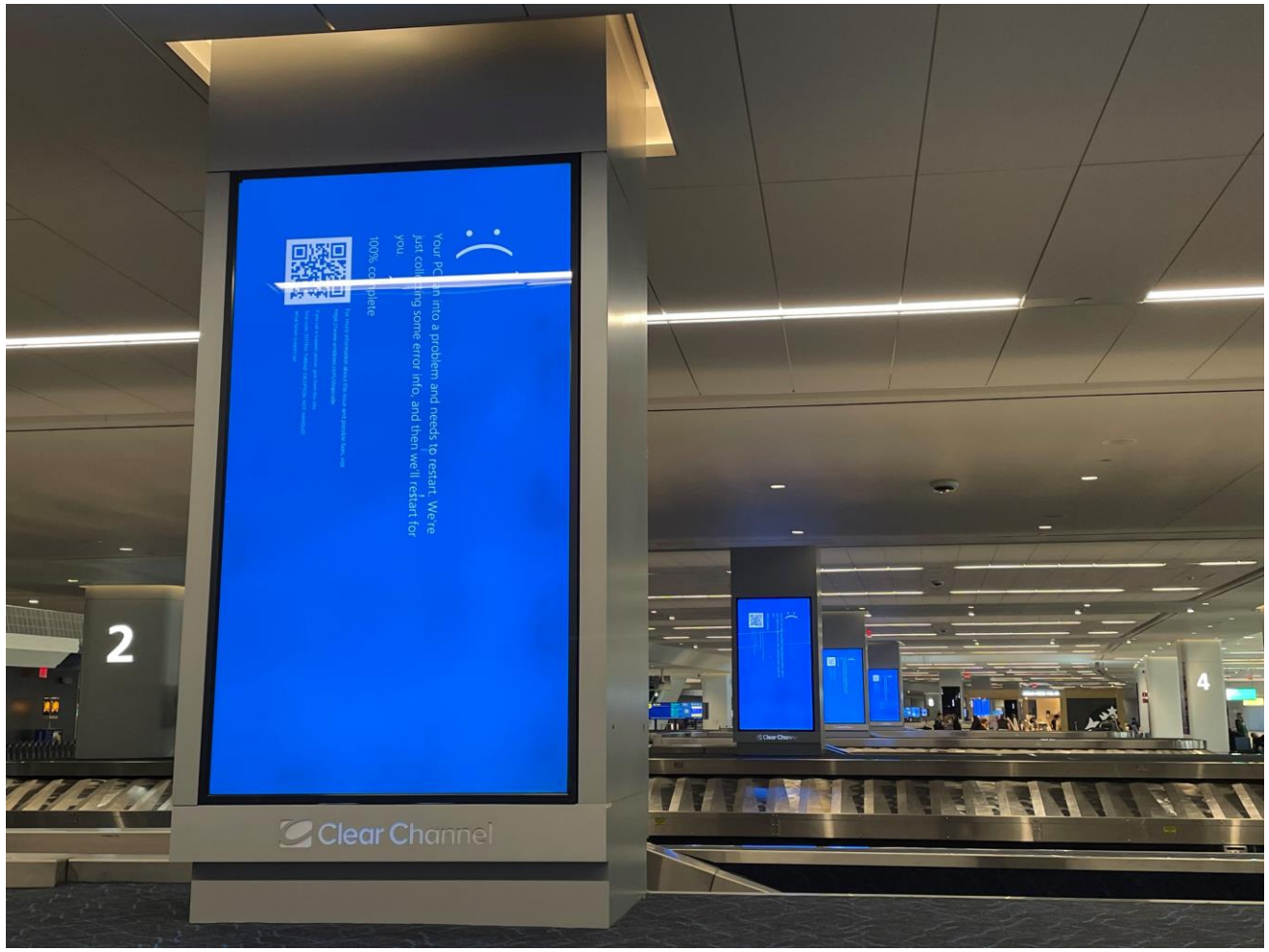
DukeHealth

macy's

DELTA

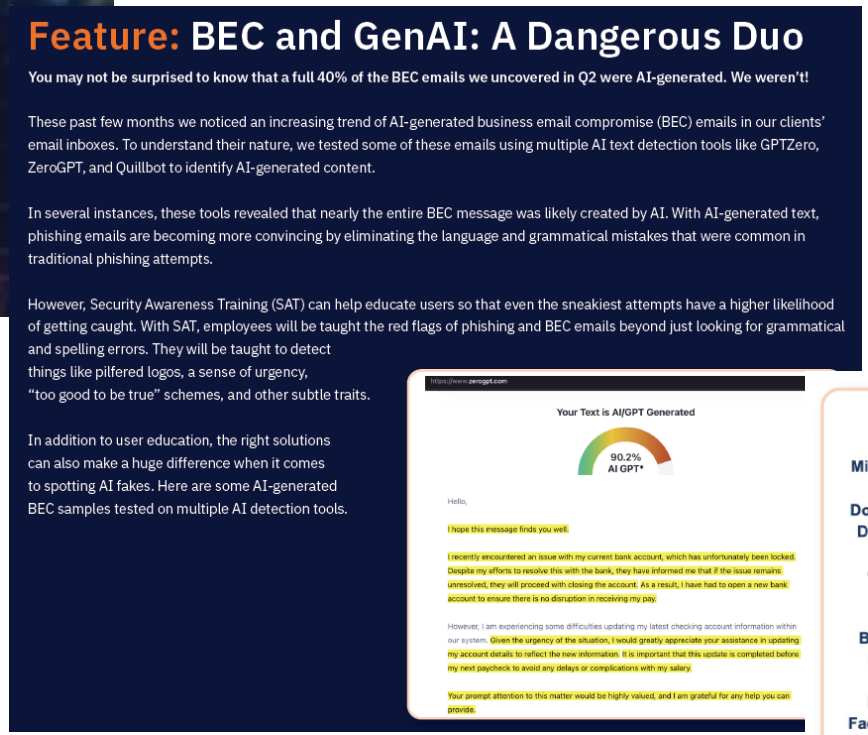
THE HOME DEPOT

Microsoft

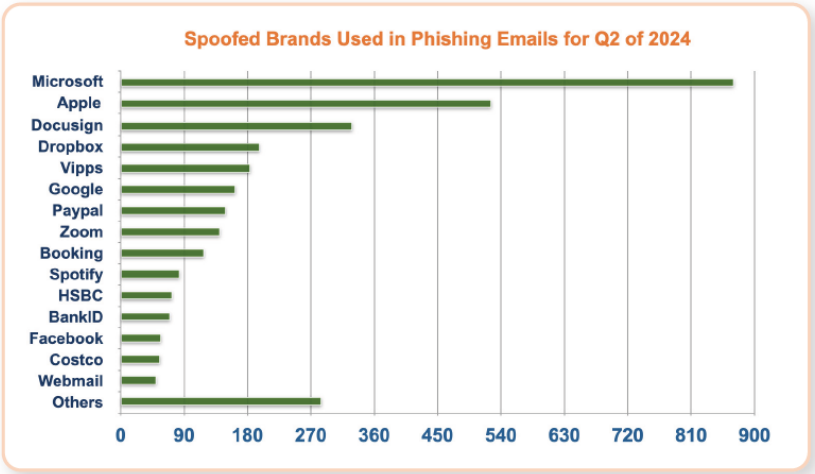


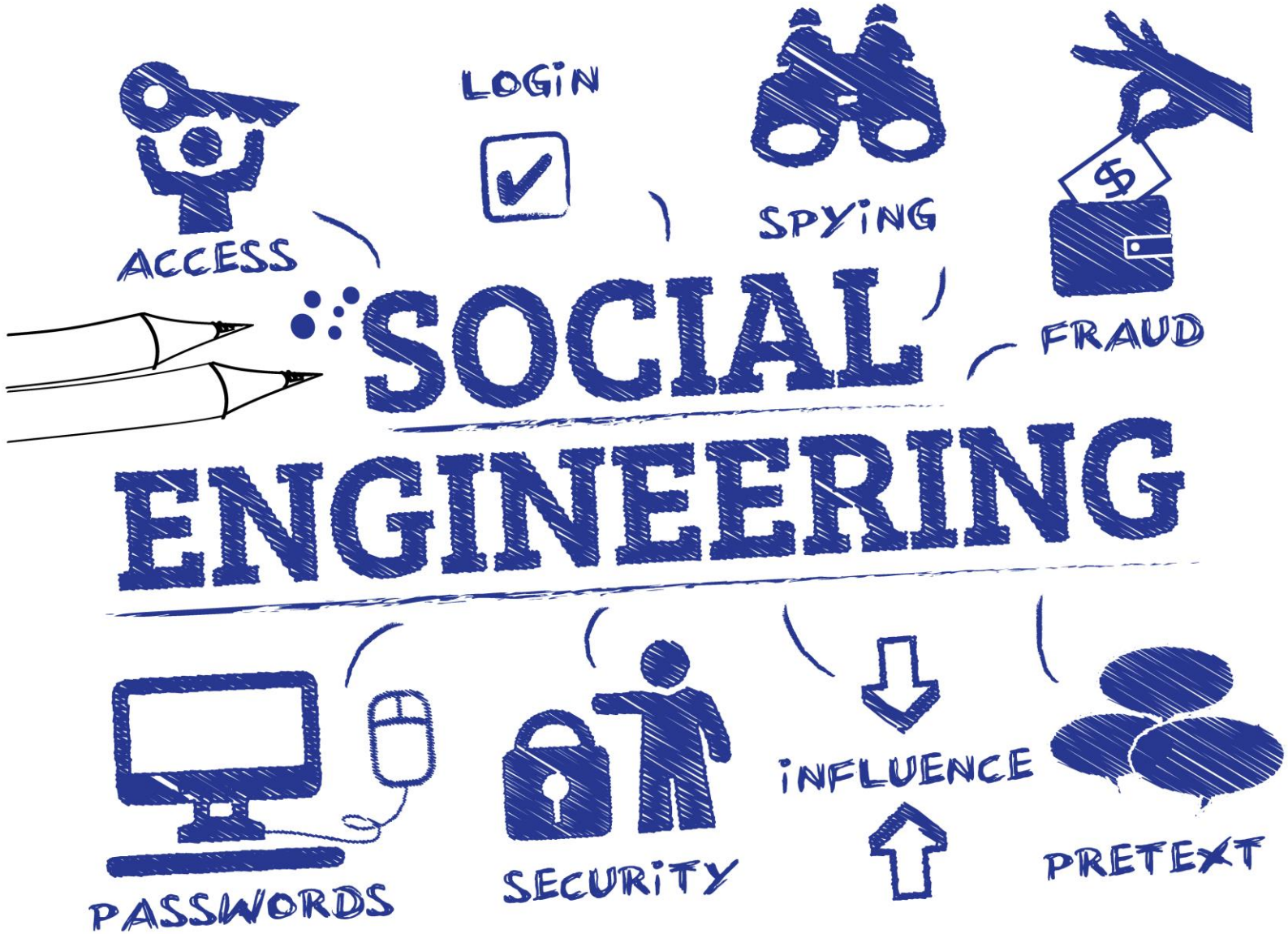
THE STATS AND EXPERTS ALL AGREE…

Source: https://socradar.io/phishing-in-2024-4151-increase-since-chatgpt/



Source: VIPRE Email Threat Trends Report Q2 2024




LOGIN
SPYING
ACCESS
SOCIAL
FRAUD
ENGINEERING
INFLUENCE
PASSWORDS
SECURITY
PRETEXT

AI POWERED SOCIAL ENGINEERING

Social Mapping

- Social mapping is a process used to visualize and analyze the social structures and relationships within a community or group.
- It helps identify key influencers, detect patterns, predict future dynamics, and visualize complex relationships in real-time.

Voice Cloning and Deepfakes

- Using AI to create synthetic voices that can be changed in real-time sounding nearly identical to the target, but each party hears what the attacker wants them to hear.
- Deepfakes can be used in fake video conferences or announcements from executives and are increasing in sophistication to the point they are nearly indistinguishable from the real thing.

AI POWERED SOCIAL ENGINEERING

Impersonation Attacks

- **Social Media Impersonation:** Using AI to create and manage fake social media profiles to gather information and launch targeted attacks.
- **Executive Impersonation:** Crafting highly realistic fake identities to impersonate executives and request sensitive information or authorize transactions.

Enhanced Spear Phishing

- **Behavior Analysis:** Leveraging AI to analyze the behavior and communication patterns of targets to create more convincing spear-phishing attacks.
- **Multi-Stage Attacks:** Orchestrating complex, multi-stage phishing campaigns that evolve based on the responses and actions of the targets. These attacks may come by multiple vectors (email, phone, SMS, etc.)

AI isn't going to replace your job - but someone using AI will

CYBERSECURITY & YOUR ORGANIZATION

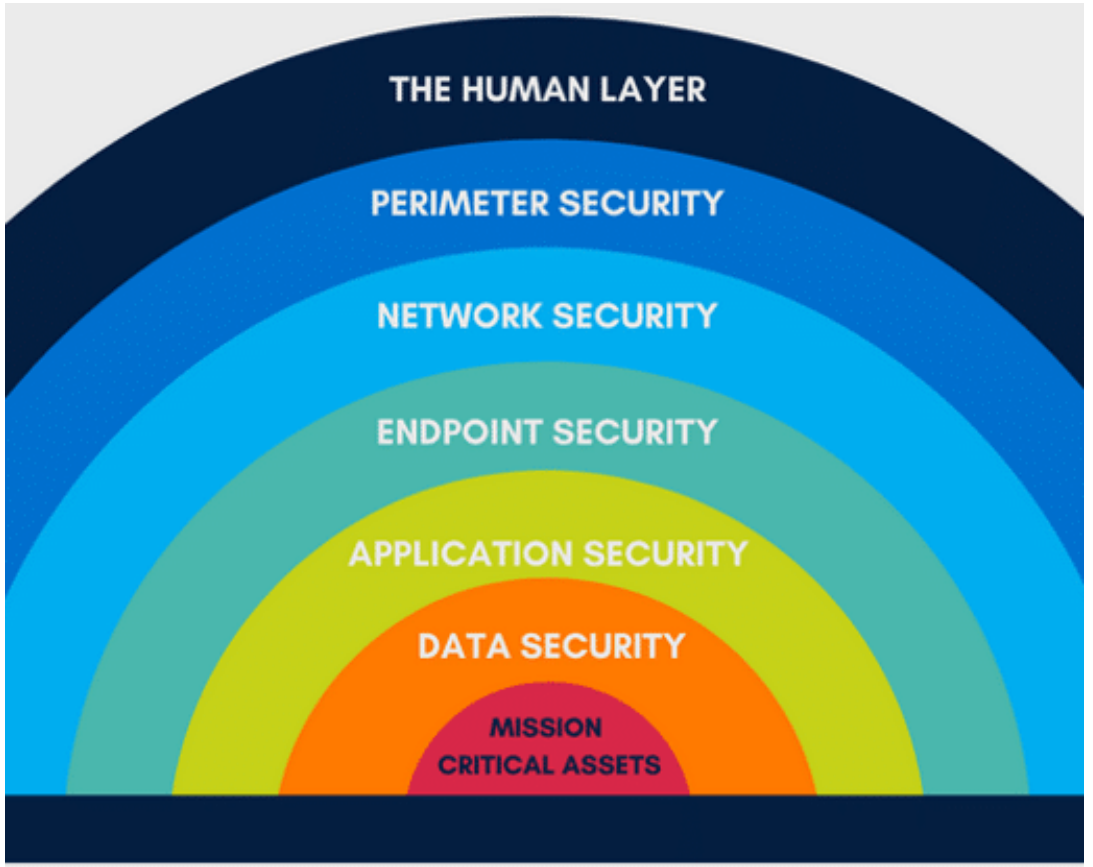
Image generated by AI using OpenAI's DALL-E engine

Home Security Layers: A Simple Analogy

- ✓ Fencing and Gates
- ✓ Exterior and Interior doors/locks
- ✓ Motion Activated Lighting
- ✓ Window Locks
- ✓ Monitoring System(s)
- ✓ Safe(s)

CYBERSECURITY & YOUR ORGANIZATION

Image generated by AI using OpenAI's DALL-E engine



Source: https://www.diamondit.pro/7-layers-of-cybersecurity/

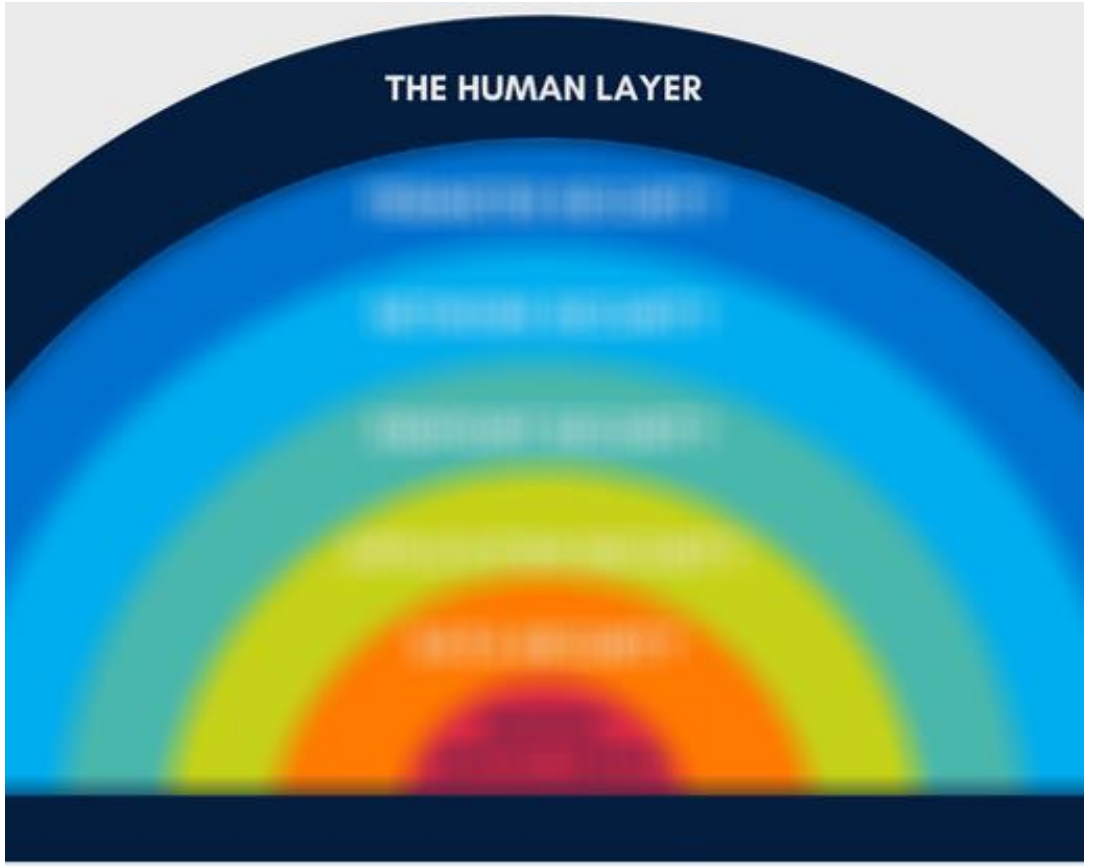
CYBERSECURITY & YOUR ORGANIZATION

Your Organization's #1 asset

- Your people are your biggest vulnerability
- Do your employees understand "the why"?

Phishing and Security-based Training

- Make it consistent and celebratory
- Awareness is the #1 driver of behavior change!

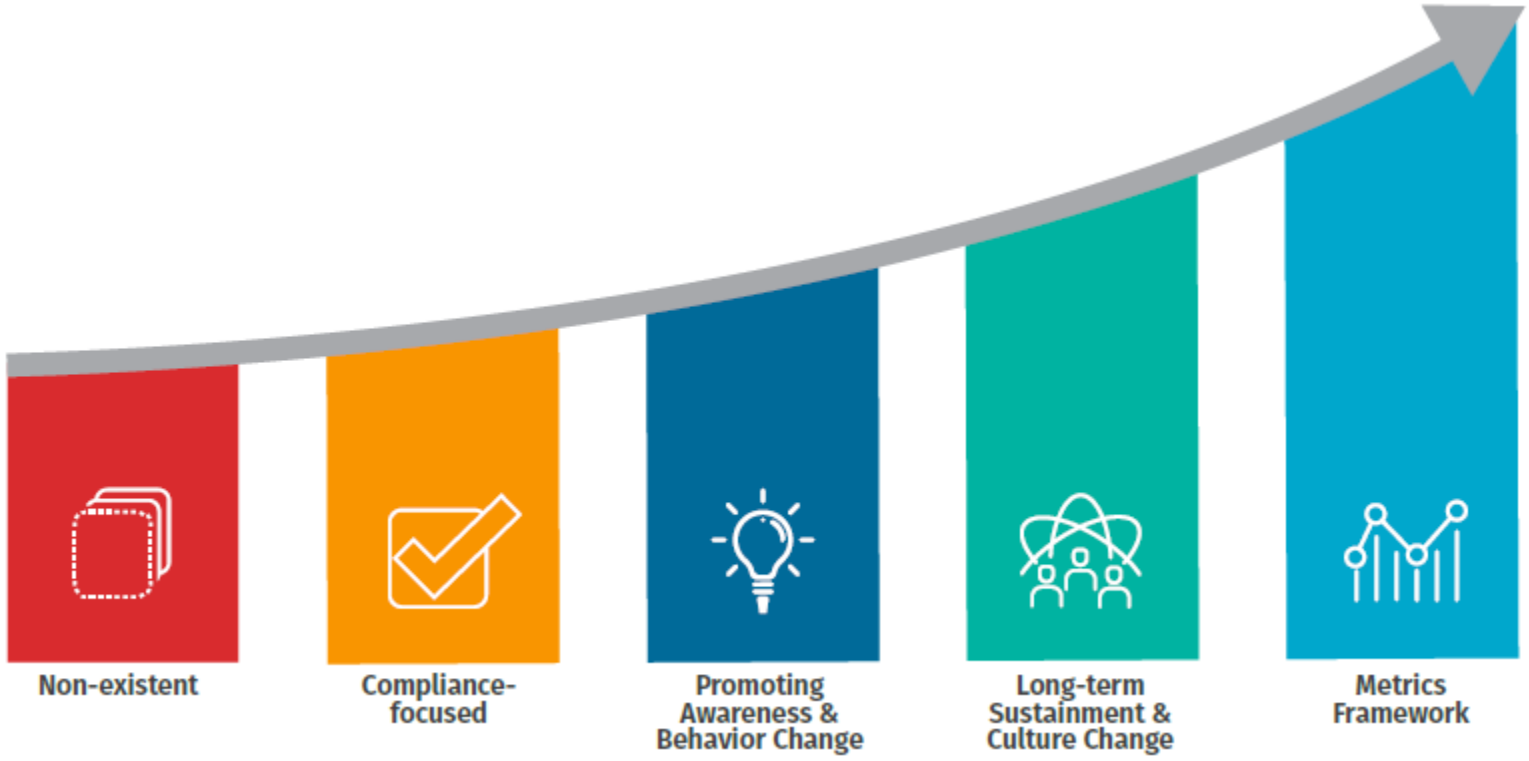


Source: https://www.diamondit.pro/7-layers-of-cybersecurity/

BUILDING A SECURITY FIRST CULTURE

A STRATEGIC APPROACH TO SECURITY CULTURE

BUILDING A SECURITY FIRST CULTURE



Source: SANS Security Awareness Maturity Model - https://www.sans.org/security-awareness-training/resources/maturity-model/

BUILDING A SECURITY FIRST CULTURE

Leadership and Management Buy-In

1. **Lead by Example:** Ensure that executives and managers visibly prioritize cybersecurity. When leadership is actively involved in security initiatives, it sets the tone for the organization.
2. **Communicate the Importance:** Regularly communicate why security is critical, not just for the organization, but for employees personally (e.g., protecting their personal data and job security).

Having Honest Conversations

- Has leadership bought-in?
- Do we understand “the why”?
- What’s our organization’s tolerance for risk?
- Do you have the right people (or partner) to build this out?
- Is there a budget?

BUILDING A SECURITY FIRST CULTURE

Foster a Culture of Accountability

1. **Empower Employees:** Make everyone feel responsible for security by emphasizing that it's not just the IT department's job. Encourage employees to report suspicious activities or potential security breaches without fear of repercussions.
2. **Regular Feedback:** Provide feedback on how well the organization is doing in terms of security. Share success stories, as well as areas for improvement, so everyone feels involved in the organization's success.

Intentional Education

- Integrate 'InfoSec' training into the new-hire process.
- Don't overload with text, instead embrace the learning styles and make the training interactive by mixing it up with picture, video and engage your audience.
- Create your own content, customize it for your organization.

BUILDING A SECURITY FIRST CULTURE

Make it Personal

1. **Relate to Personal Life:** Highlight how good cybersecurity practices at work can also benefit employees in their personal lives. Encourage employees to share what they learn with family and friends.
2. **Incentives and Rewards:** Introduce incentives for good security behavior, such as recognizing employees who spot phishing attempts or adhere to security best practices.

What's in it for them?

- Employees who follow good security practices help protect the company.
- Good security habits protect their personal information from being compromised, both at work and at home.
- Understanding and practicing cybersecurity is increasingly becoming a valuable skill set. Employees can enhance their careers by gaining knowledge and contributing to the organization's security efforts.

BUILDING A SECURITY FIRST CULTURE

Security is everyone's job, we all play an important role in our organization and in our spheres of influence. WE CAN CREATE A CULTURE OF SECURITY!

Build a security awareness training program across your organization. Many free resources exist and some organizations provide free videos, activities, print material and more.

- If you already have a program in place consider making employees aware of all the types of data that your organization retains and that they're protecting.
- Security awareness starts with basic principles of psychology, if you can get your employees emotionally invested, it becomes more meaningful and long lasting.
- We need to have positive messaging to make security stick, not "Death by PowerPoint". Changing the way we communicate information to our employees is the key to success.

FINANCIAL FRAUD KILL CHAIN (FFKC)

- ✓ It's a process to help recover large international wire transfers stolen from the United States.
- ✓ The FFKC is intended to be utilized as another potential avenue for U.S. financial institutions to get victim's funds retuned.
- ✓ The FFKC can only be implemented if the fraudulent wire transfer meets the following criteria:
  - The wire transfer is $50,000 or above
  - The wire transfer is international
  - a SWIFT recall notice has been initiated
  - The wire transfer has occurred within the last 72 hours (the sooner the better)

How to initiate the "kill chain" if a BEC event occurs

1. Call the bank
2. Call the local police and file a report
3. Call the Secret Service or FBI in your local district and tell them you would like to talk to someone to "File a Kill Chain".
4. They will initiate the process and ask for all documentation (the police report will come later) in digital format to be provided.

IMPORTANT NOTE: ***Time is of the essence and every minute counts, it's advisable to have a SOP built out for scenarios like this.***

NEXT STEPS – ACTION ITEMS

- **Create a Security Awareness Training and Employee Education Program**
  - Look for training platforms that focus on employee education.
  - Many tools integrate with Outlook making it easy to report phishing and alert IT.

- **Designate someone responsible for security in your organization**
  - This should be an employee who owns this for the organization. It can also include a trusted partner/vendor.

- **Create an AI Acceptable Use Policy (AUP) for your organization**
  - Establish the purpose and explain the goals in promoting ethical AI use.
  - Provide clear rules for use and address privacy and security concerns.

NEXT STEPS – ACTION ITEMS

- **Perform a baseline/security assessment with a trusted partner.**
  - Review results to determine priorities, gaps and dependencies.
  - Regroup with your team including executives from different areas, not just IT.
  - Create a roadmap, track progress, review regularly and continuously evolve.
  - Review data classifications within Microsoft 365 before rolling out Copilot.

- **Create an Incident Response Plan (IRP) for your organization**
  - Be sure to test this regularly and run scenarios following your IRP.
  - This may consist of a handful of scenarios not all technical; called playbooks.
  - This is a great opportunity for organizational alignment to the security mission.

THANK YOU

- J.D. Mulliken
- 717-695-1840
- email@jdmulliken.com
- www.jdmulliken.com

SCAN ME