CYBERSECURITY RISK & SOCIAL ENGINEERING: EMPOWERING FINANCE TEAMS TO NAVIGATE THE HUMAN FACTOR

Danny Sementilli III

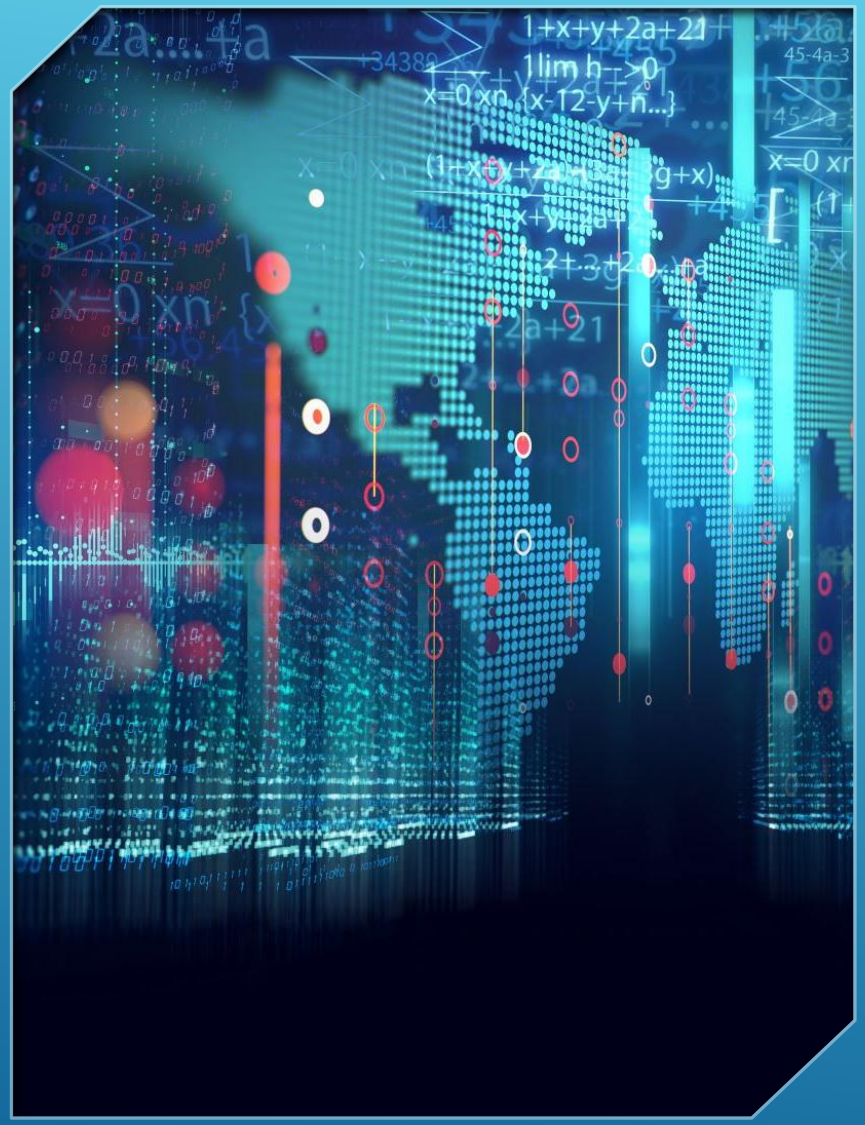
City of Coconut Creek IT Director

dsementilli@coconutcreek.gov

INTRODUCTION - WHOAMI

- Environment
  - Heavily Virtualized ~110 servers
  - Maintain dark fiber network city wide
  - Oversee all infosec aspects (Firewall, Vulerability Scanner, End-point detection, MFA etc.)
- 14 Full Time Staff
- Support ~500 city employees across multiple locations

- Cybersecurity is crucial for municipal trust and digital resilience in local governments.
- We understand the technical landscape, but today we are focusing on the human layer – the most difficult threat vector to defend against.
- Attackers are increasingly targeting the human element rather than solely exploiting technical vulnerabilities. This shift in threat dynamics underscores the necessity of educating finance personnel, who play a vital role in safeguarding municipal operations



TODAY'S AGENDA:

-THE THREAT

-THE PSYCHOLOGY

-THE DEFENSE

-THE PARTNERSHIP

THE THREAT - WHY FINANCE IS THE PRIMARY TARGET

High Risk Finance Access

Finance departments handle liquid funds and urgent transactions, making them prime cyberattack targets.

Human Factor Vulnerabilities

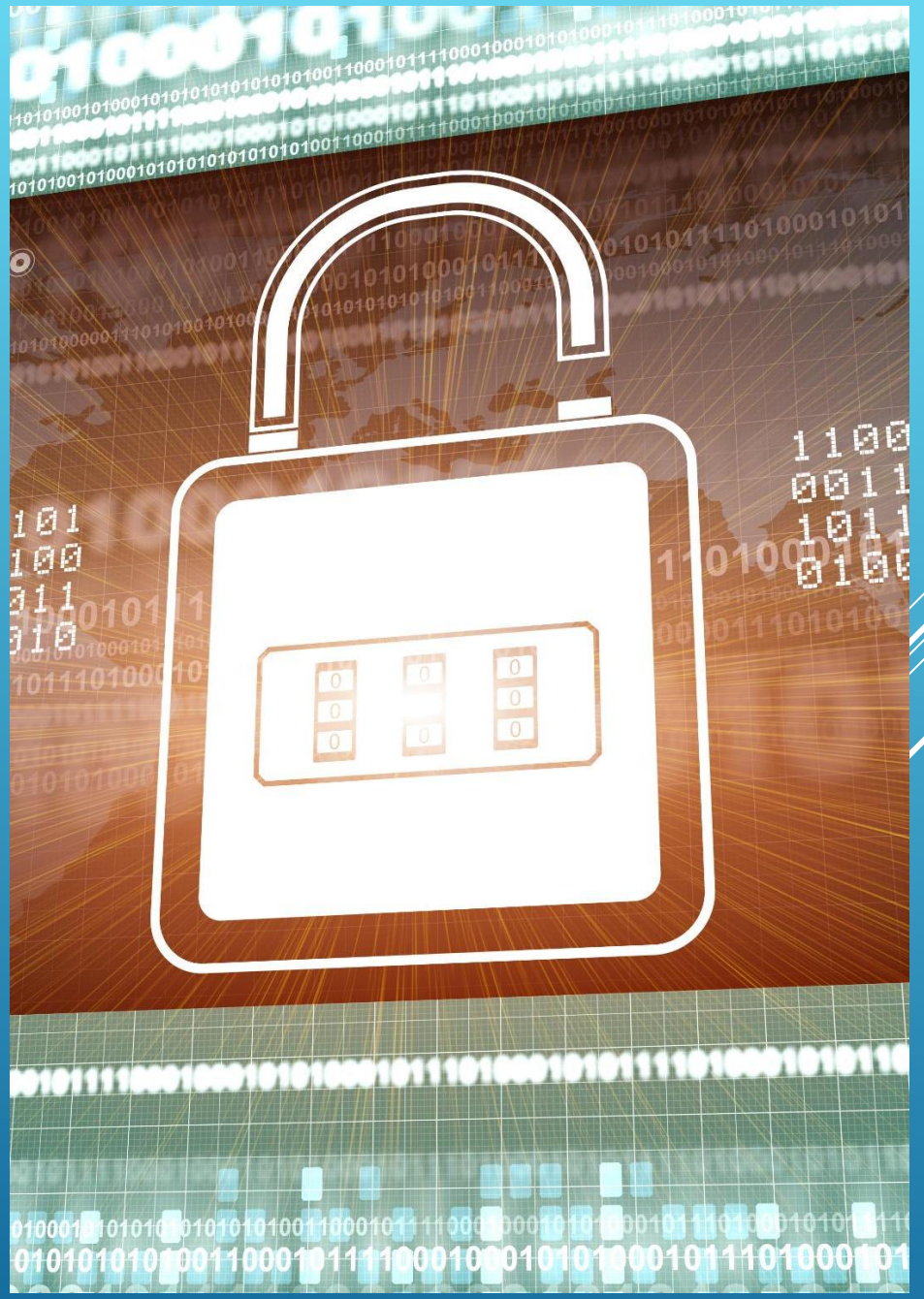
82% of breaches involve human error or manipulation, highlighting behavioral exploitation over technical flaws.

Sophisticated Social Engineering

Attackers impersonate trusted partners or officials, using social engineering to bypass traditional defenses.

Complex Municipal Ecosystem

Municipal finance operates within strict timelines and vendor ecosystems, creating exploitable predictable patterns.



THE PSYCHOLOGY OF SOCIAL ENGINEERING

Cognitive Vulnerabilities

Human brains are optimized for efficiency, making people susceptible to authority, urgency, and trust cues used by attackers.

Common Attack Techniques

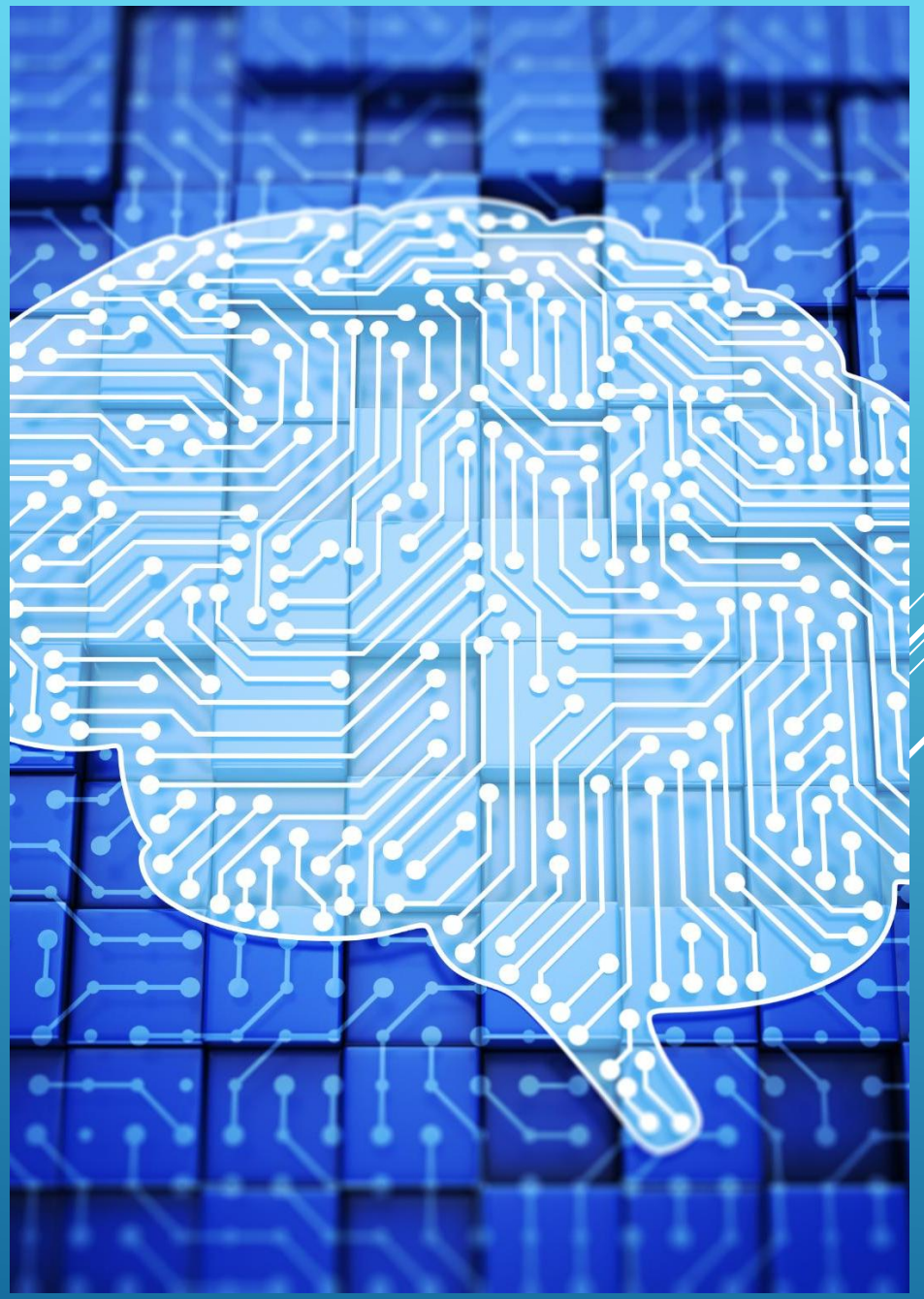
Attackers impersonate executives, create false deadlines, or pose as vendors to manipulate targets effectively.

Targeted Vulnerable Groups

Finance staff are targeted because their responsiveness and helpfulness can be exploited during stressful periods.

Importance of Awareness

Recognizing psychological vulnerabilities is crucial as technical defenses alone cannot prevent all social engineering attacks.



ANATOMY OF THE ATTACK – WHAT IT LOOKS LIKE

Compromised Vendor Accounts

Attackers infiltrate legitimate vendor accounts to send fraudulent banking requests at opportune moments.

CEO Fraud and Email Compromise

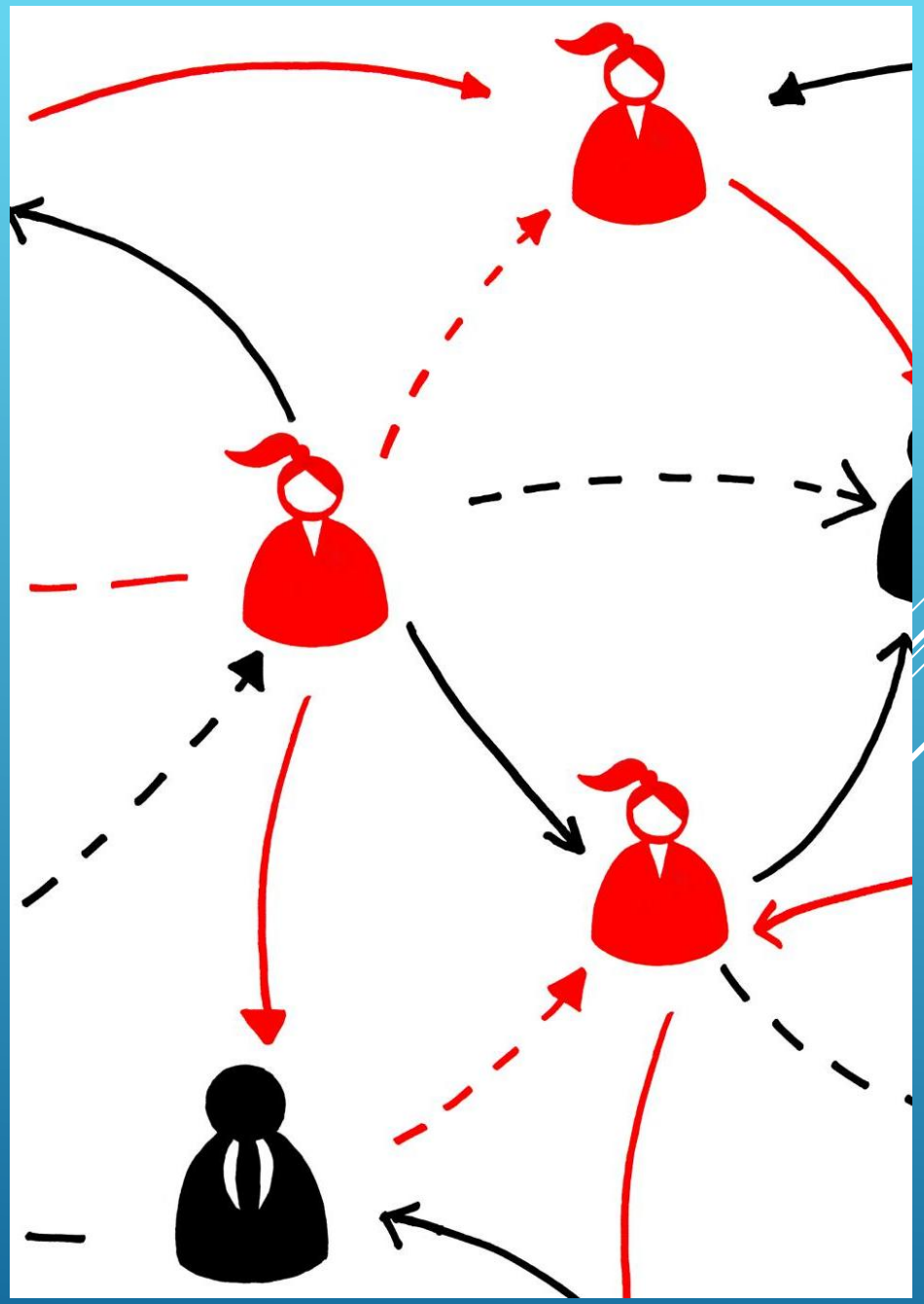
Fraudsters impersonate executives to pressure employees into executing illegitimate financial transactions.

Fraudulent Invoices and Attachments

Malicious attachments and counterfeit invoices mimic routine documents to deceive recipients.

Human Error and Vigilance

Even with security tools, human vigilance is critical to spotting subtle red flags in phishing emails.



EXAMPLES OF SUCCESSFUL ATTACKS

- **1. The $25 Million "Deepfake" Wire Transfer (Hong Kong, Feb 2024)**
  - **The Attack:** Finance staff at a multinational company participated in a video conference call with what appeared to be the company's CFO, CEO, and other executives. The participants were **AI-generated deepfakes**. The real executives were not on the call.
  - **The Trick:** The scammers used deepfake audio and video to mimic the voices and faces of senior leadership. They created a sense of urgency and legitimacy that bypassed the finance team's normal skepticism.
  - **The Result:** The finance team transferred **$25.6 million** to a fraudulent account before realizing the call was fake.
  - **Lesson for Finance: Video calls are no longer proof of identity.** If a request involves a large wire transfer, it must be verified via a secondary, pre-established channel (e.g., a known phone number), regardless of how real the video looks.
- **Source:**
  - https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk
  - https://www.linkedin.com/pulse/he-verified-video-call-lost-25-million-marcos-lima-g6wrc

EXAMPLES OF SUCCESSFUL ATTACKS

- **2. The MGM Resorts Cyber Breach (Las Vegas, September 2023)**
  - **The Attack**: A hacking group called "Scattered Spider" (also known as UNC3944) breached MGM Resorts International's systems, paralyzing operations across their network of over 30 hotel and gaming venues worldwide, including locations in Las Vegas and Macau.
  - **The Trick**: Leveraged social engineering tactics to lure employees into surrendering login credentials or one-time-password (OTP) codes, effectively bypassing multi-factor authentication protections. This approach proved challenging even for organizations with mature security programs to defend against.
  - **The Result**: Multiple MGM systems remained paralyzed for several days, causing significant operational disruption. Moody's rating agency warned the breach could negatively impact MGM's credit rating, citing the company's heavy reliance on technology and the operational disruption caused when systems went offline. Shares of both MGM and Caesars Entertainment fell following the incident.
  - **Lesson**: MFA alone is insufficient; prioritize security awareness training and layered verification.
  - **Source:**
    - https://www.reuters.com/technology/moodys-says-breach-mgm-is-credit-negative-disruption-lingers-2023-09-13/
    - https://conscious.net/mgm-social-engineering-attack-attacks-and-lessons-learned/

THE DEFENSE - BUILDING A HUMAN FIREWALL

Stop, Look, Verify Protocol

Pause before responding, inspect sender details, and verify changes through trusted channels to prevent fraud.

Out-of-Band Verification

Always use separate communication channels for validation to enhance payment security and reduce risks.

No-Blame Reporting Culture

Encourage timely reporting by avoiding punitive measures, fostering openness to detect and prevent fraud.

Technical and Training Support

Use multi-factor authentication, email filtering, and structured training to strengthen human firewall defenses.

THE PARTNERSHIP - BRIDGING THE GAP BETWEEN IT AND FINANCE

Collaboration Importance

Close collaboration between IT and Finance is essential for secure financial operations.

Understanding Financial Cycles

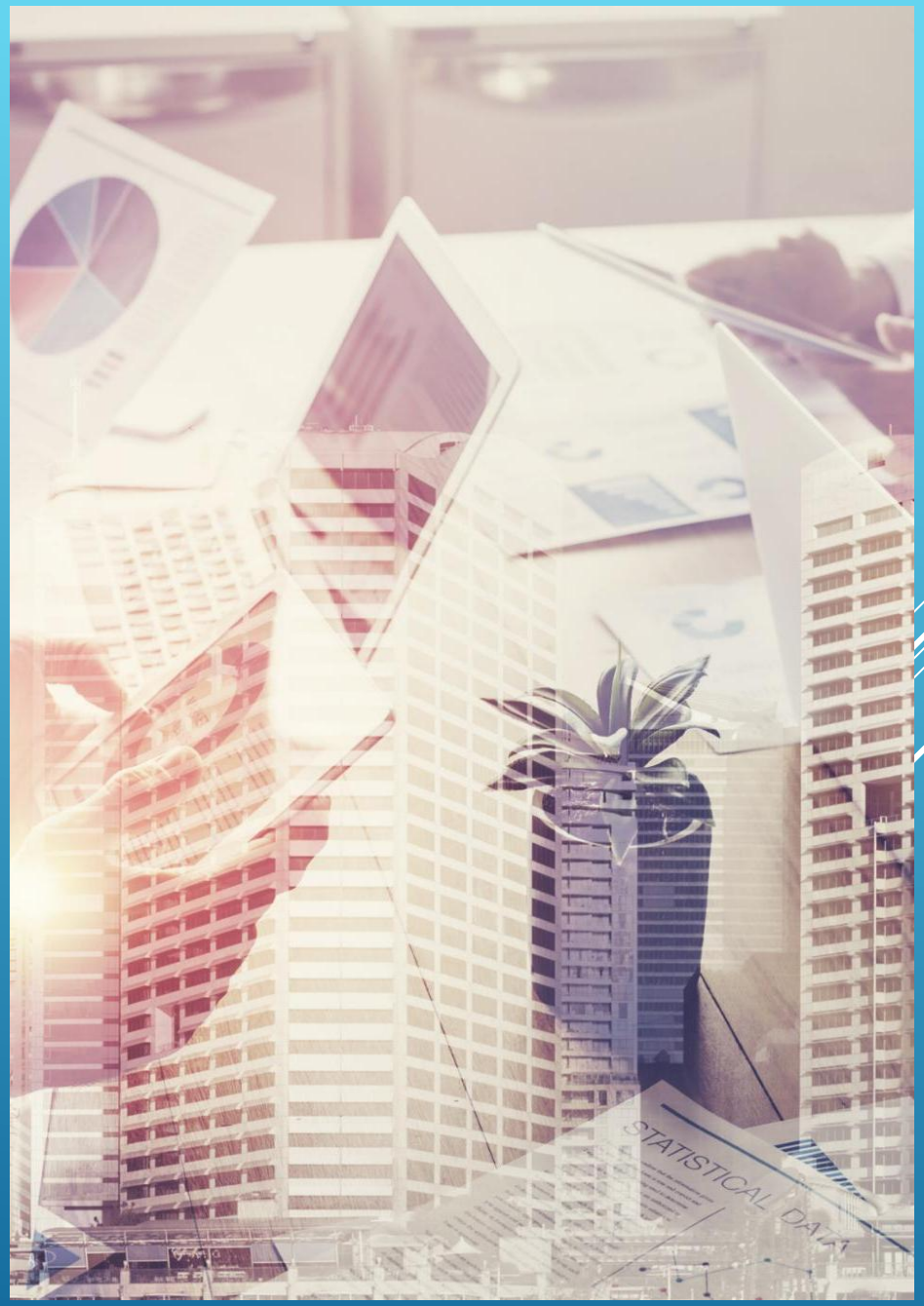
IT must recognize high-pressure financial cycles like month-end to tailor security alerts effectively.

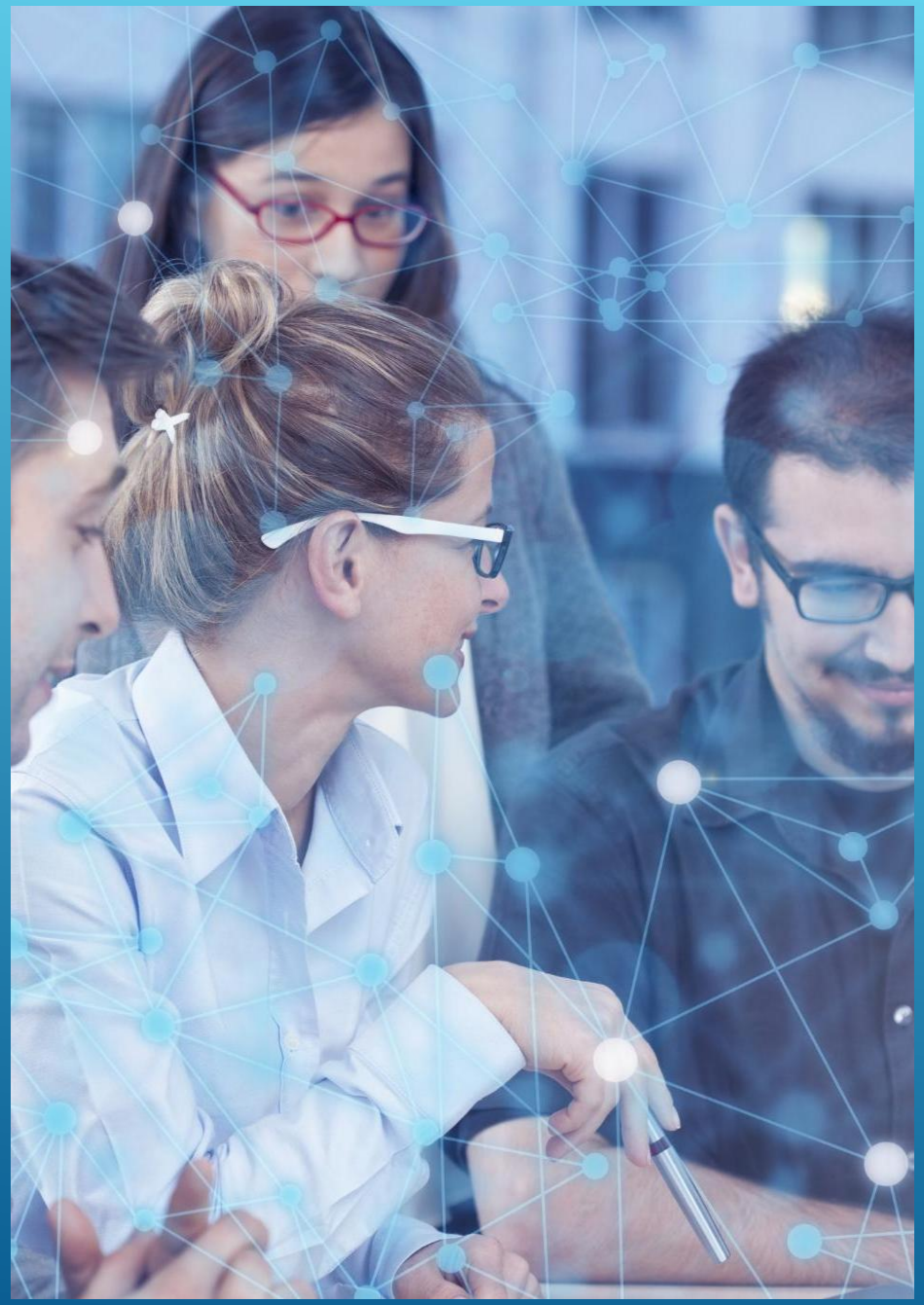
Joint Security Drills

Role-specific phishing simulations and drills enhance preparedness and reveal vulnerabilities.

Shared Accountability

Mutual trust and shared responsibility create a unified defense protecting critical services.





A CALL TO ACTION

Urgency of Defense

Social engineering attacks are real, growing in sophistication, and target human behavior more than technology.

Verify Before You Pay

Adopt the 'Verify Before You Pay' rule to prevent most fraudulent transactions involving banking information.

Training and Collaboration

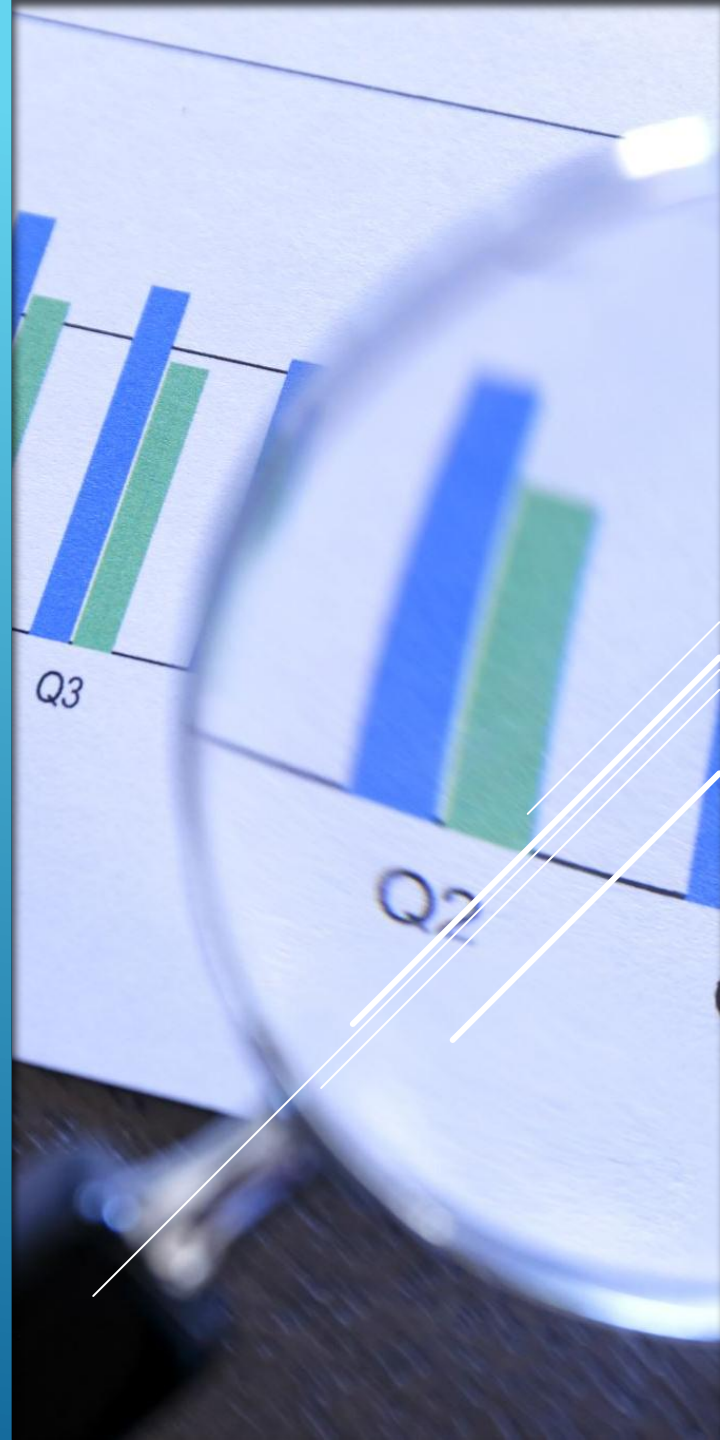
Continuous training and cross-department collaboration are essential to maintain proactive security awareness.

Empowering Staff

Empowered staff transform from vulnerabilities into defenders, protecting organizational integrity and mission.

REFERENCES & FURTHER READING

- **Industry Standards & Statistics**
  - **Verizon Data Breach Investigations Report (DBIR) 2024**
    - *Focus:* Human element statistics and breach patterns.
    - www.verizon.com/business/resources/reports/dbir
  - **FBI Internet Crime Report 2023 (IC3)**
    - *Focus:* Financial losses from Business Email Compromise (BEC).
    - www.ic3.gov/Media/PDF/AnnualReport/2023/IC3AnnualReport2023.pdf
  - **Anti-Phishing Working Group (APWG) Trends Reports**
    - *Focus:* Quarterly phishing volume and trend analysis.
    - apwg.org/trendsreports
- **Government Guidelines & Frameworks**
  - **CISA "Shields Up" Guidance**
    - *Focus:* Actionable cybersecurity guidance for critical infrastructure and local government.
    - cisa.gov/shields-up
  - **NIST Special Publication 800-50**
    - *Focus:* Building an Information Technology Security Awareness and Training Program.
    - csrc.nist.gov/publications/detail/sp/800-50/final
  - **Florida Local Government Resources**
  - **Florida Dept. of Management Services (DMS) Cybersecurity**
    - *Focus:* State-level cybersecurity initiatives and resources for FL agencies.
    - dms.myflorida.com/workforce_operations/cybersecurity
  - **Florida League of Cities Cyber Toolkit**
    - *Focus:* Practical tools and best practices for Florida municipalities.
    - flcities.com/cybersecurity




QUESTIONS?