Building Cyber Resilience Against Social Engineering Attacks

Speaker: Bharat Bajaj and Puneet Tikoo

CISO Melbourne : 22 July 2025

Who are we?

Bharat Bajaj

An experienced Technology risk partner with a career spanning two decades in the financial industry.

Background:-

Artificial Intelligence, Machine Learning, Cyber Security and Privacy domains.

Profession:-

Post-nominals include CRISC, CISM, CDPSE, ITIL & Six Sigma.

Puneet Tikoo

GRC specialist and worked within Financial, Defense and Consultancy areas

Background:-

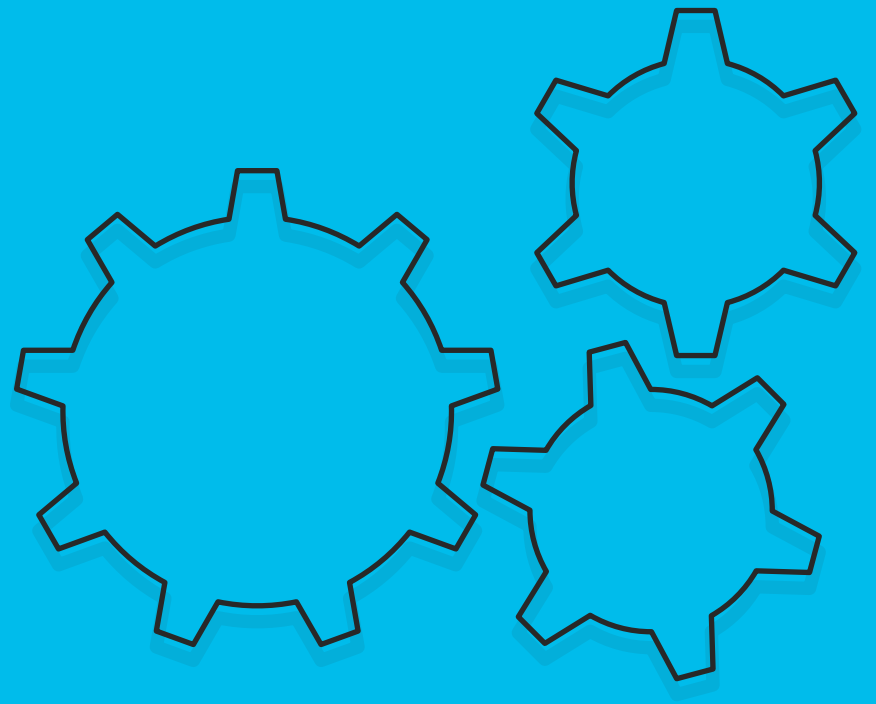
Infrastructure, Cloud, Governance Risk and Compliance (GRC)

Profession:-

CISSP, CISA, CCSP, IRAP Assessor, ISO27K1 Lead Auditor

Agenda Overview

1. Story of a Scam Victim / Worker
2. Understanding Social Engineering Attacks
3. TALOS Report (Annual review 2024)
4. Practical guidance for the business



Story of a Scam Victim

Victim or Perpetrator

Department of Justice (.gov)
https://www.justice.gov › usao-ks › former-ceo-failed-b...

Former CEO of failed bank sentenced to prison

19 Aug 2024 — "**Shan Hanes** was sentenced today for his role in a $47.1 million embezzlement scheme that ultimately caused Heartland Tri-State Bank to fail," ...

CNBC
https://www.cnbc.com › 2024/08/21 › cryptocurrency-s...

Crypto scam wrecks Kansas bank, sends CEO to prison

21 Aug 2024 — Heartland Tri-State Bank in Kansas failed after **CEO Shan Hanes** caused $47 million in wire transfers to be sent to scammers running a pig ...

Timelines

2022

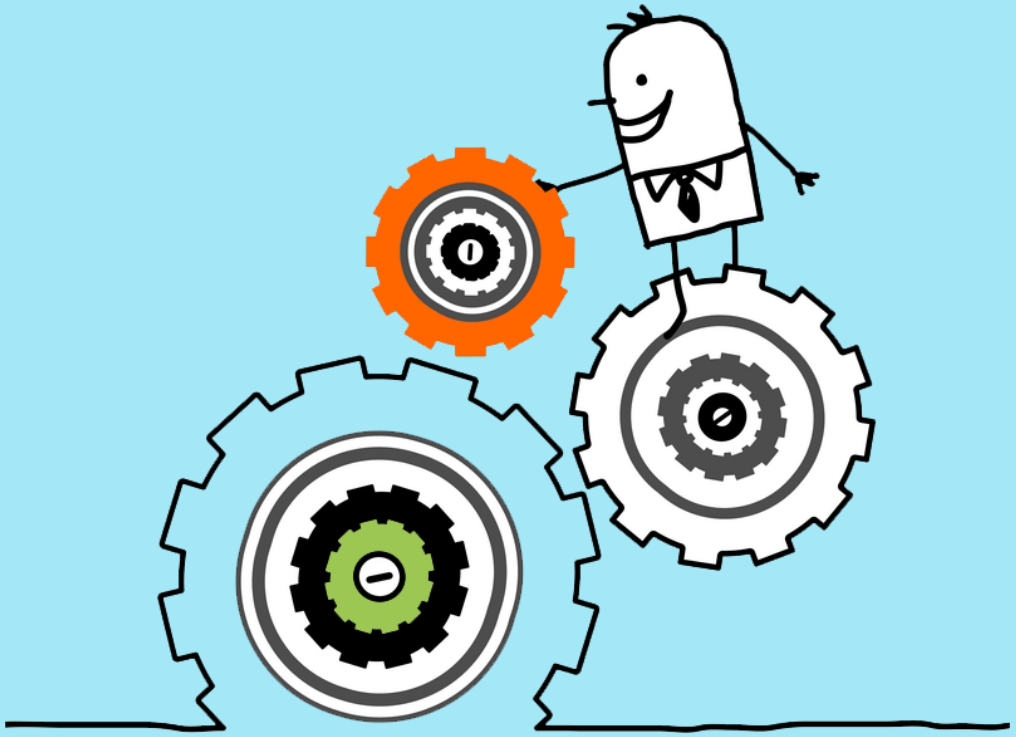
- CEO of Heartland Tri-State Bank
- Chairman of the Kansas Bankers Association
- Frequently testified before Congress on important topics
- Board members Heartland Tri-state bank worried that Shane would leave for a bigger bank or become a Washington lobbyist.

2023

- $40,000 from Elkhart Church of Christ
- $10,000 from the Santa Fe Investment Club
- $60,000 from his daughter’s college fund
- $1 million in stock from the Elkhart Financial Corporation
- 11 wire transfers totaling $47.1 million of Heartland’s funds to a cryptocurrency wallet
- $18 million requested and argued this would yield a $20 million profit.

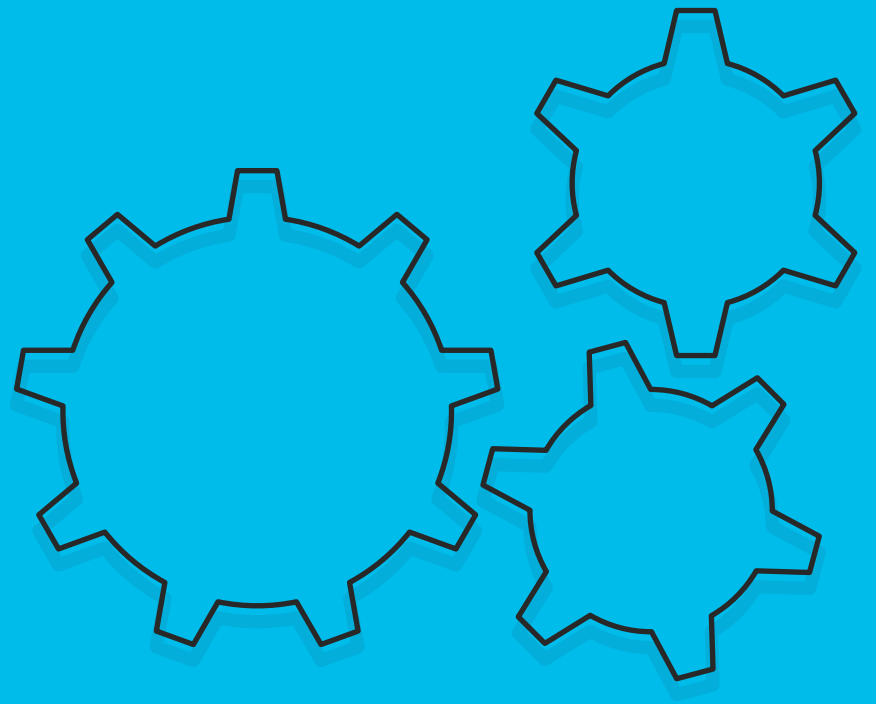
2024

- Jailed for 23 years for embezzlement

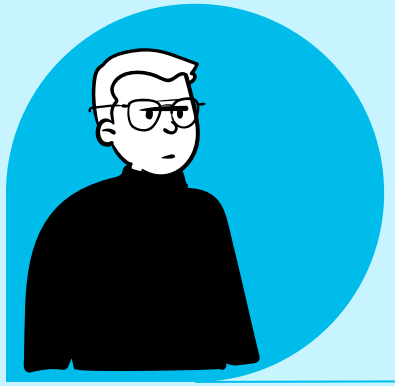


What is the Pig Butchering Strategy?

Pig butchering fraud is a **slow-burn** social engineering scam in which attackers build **fake relationships** with victims before executing financial theft, often through fraudulent investment platforms. The name comes from the Chinese phrase sha zhu pan, which refers to "**fattening the pig before slaughter**."



Story of a Scam Worker



Mr. Kumar

Age: 24 yr

Location: Maharashtra, India

Education:-

- Bachelor Degree in computer science

English Proficiency:-

- Professional Speaking

Job Medium:-

- Social Media Platform

Proposed Job:-

- A high paying computer teacher in Bangkok.
  Joined the centre: August 2022

Life of a scam worker

TOOLS

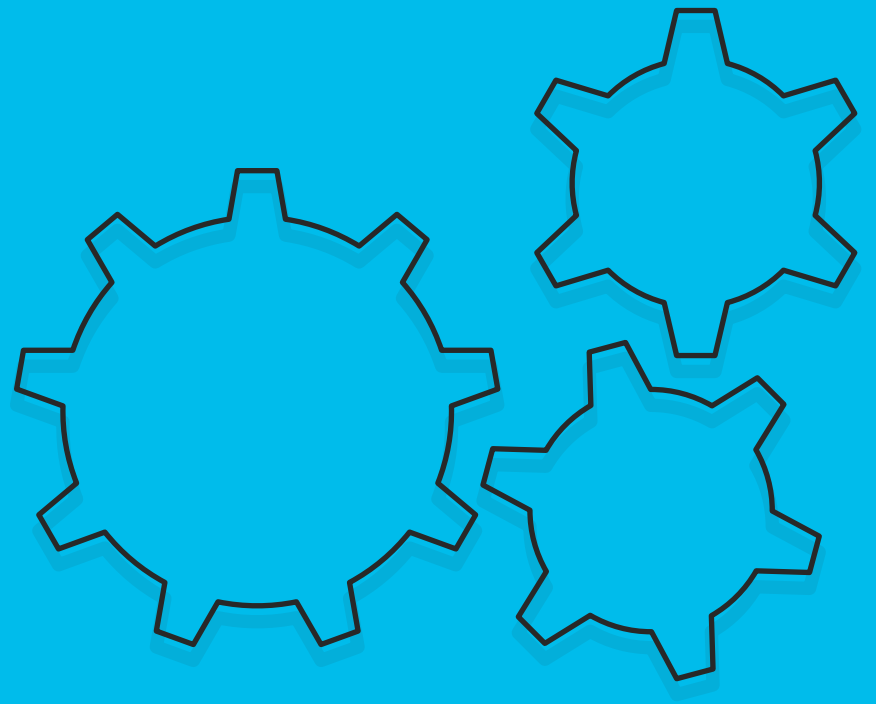
IDENTITIES

TRAINING

WORKING CONDITION

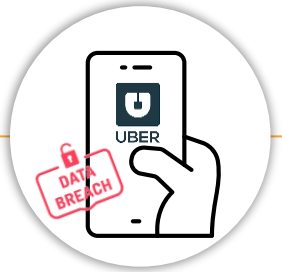
WORK REFUSAL

EXTORTION



Social Engineering Attacks

Cyber Attacks – Social Engineering incidents



Uber Data Breach

- Password of Uber employee was obtained from the dark web marketplace
- **MFA flooding (Impersonating as member of Uber security via What's App)**
- PowerShell scripts contained login credential of admin user

MGM Resorts - Casino

- **Social Engineering on IT Helpdesk**
- LinkedIn impersonation
- 100 million loss (No ransom was paid – loss in business)
- 100+ ESXi servers were encrypted

Okta

- **Social engineering attacks designed to steal privileged credentials**
- Employees Gmail account was compromised. It was logged into company laptop and passwords saved in Chrome
- Malware installed on the laptop

Talos (Year in Review Report – 2024)

TALOS Report

1. 46 million devices across 193 countries
2. 60% incidents in 2024 were focused on **identity-based** attacks
3. Most Targeted Vulnerabilities – Misconfigured systems, MFA weakness
4. Unpatched Systems
5. 4 out of top 12 vulnerabilities in 2024 were published a decade ago
6. Top tools used by attackers – PsExec, **PowerShell**, Mimikatz and RDP
7. Vulnerabilities affecting end-of-life (EOL) devices are amongst most targeted network device CVEs
8. Adversaries gained initial access via **phishing in nearly a quarter of Talos Incident Response (IR) incidents**

Practical Guidance for the Business

1

Security Culture
Cyber-security is a journey. Do the right thing and don't treat cyber as a tick-box exercise. Adhere to required frameworks and keep on improving cyber security posture

2

Physical Protection
Physical certification, SCEC assessment for Datacenter cages and zones, Access cards, Wireless Access Point etc.

3

Hardware Inventory
Server equipment, Network equipment, Workstations, USBs

4

Secure Configuration (Hardware)
Firmware, Device drivers, Supply Chain

5

Software Inventory
OS versions, Application versions, Network equipment software

6

Secure Configuration (Software)
Patches for Networking equipment (Switches/Firewalls/Load Balancers) and Storage Area Networks - SANs

7

Training & Security Awareness
All staff training, customised training for admin teams, OWASP trainings for developers, empower your admins with right coaching/mentoring

8

Business Impact Analysis (BIA)
Dictates backup requirements, feeds into BCP/DRP and Incident Response Plan (IRP)

9

Password Manager
Use corporate password managers (if possible), don't save passwords in your browsers, use separate passwords (personal/works).

10

Identity & Access Management
Single Sign on (SSO), Privileged environments (Bastion Hosts), Secure Administration. **Phishing resistant MFA for admins**

11

Incident Response Plan (IRP)
Prepared and rehearsed IRP, full testing (Table-top exercise with your Board), Formulate the **Communication Plan**

Promoting Security within Business

Importance of security culture

A strong organisational culture enhances cybersecurity by encouraging a ***collective responsibility*** for security practices.

Encouraging Proactive Behavior

Fostering an environment where employees are motivated to prioritise security can lead to early detection of threats.

Reporting Suspicious Activities

Encouraging employees to report suspicious activities contributes to a safer and more secure workplace environments.

Recognising Social Engineering

Training programs focus on helping employees identify social engineering tactics, enhancing overall organisational security.

Latest Threat Landscape

Employees are informed about the latest threats in cybersecurity, ensuring they stay updated on the evolving threats.

Practical Exercises

Training includes practical exercises that simulate real-world scenarios, allowing employees to practice their response skills. **Tabletop exercises** for Incident Response, Ransomware incidents, BCP/DR scenarios (for Boards)

Conclusion

Understanding Social Engineering

- Recognising the tactics used in social engineering attacks is crucial for effective prevention and defense.

Raising Awareness

- Training and awareness programs can empower employees to recognise and respond to potential threats.

Cyber hygiene

- Organisations should adopt comprehensive security measures(technical, procedural and informational) to mitigate the risks associated with social engineering.

References:

https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/

https://www.mitnicksecurity.com/blog/uber-data-breach

https://blog.barracuda.com/2025/10/21/social-engineering-attacks--what-msps-need-to-know

https://trustedsec.com/resources/tools/the-social-engineer-toolkit-set

https://www.cyber.gov.au

https://www.bbc.com/news/articles/cw076g5wnr3o

https://www.hybrid-analysis.com/

https://www.irrawaddy.com/news/investigation/surrounded-by-fighting-a-myanmar-crime-hub-is-oddly-unscathed.html

https://www.dw.com/en/indians-trapped-in-myanmars-cyber-scam-nightmare/a-71822893

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Questions?

bharat.bajaj@isaca-melbourne.org.au

https://www.linkedin.com/in/bbajaj/

ptikoo@cisco.com

https://www.linkedin.com/in/puneettikoo/