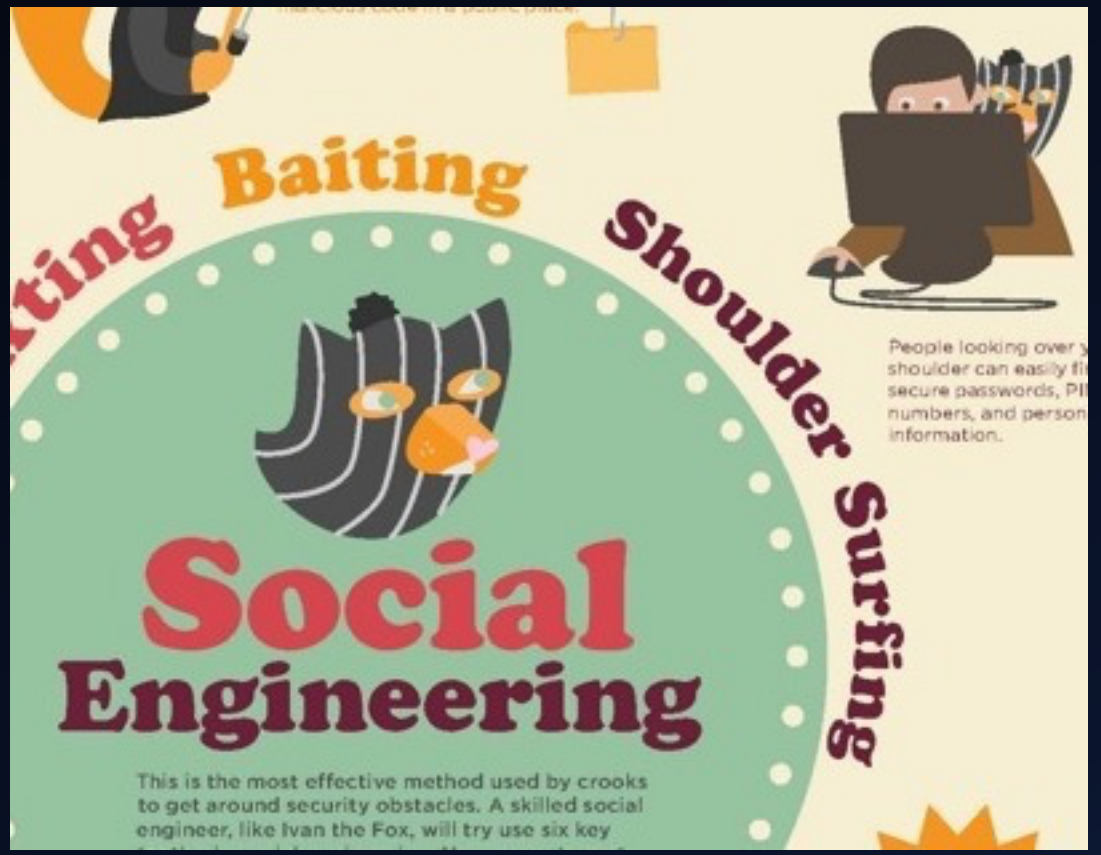
Risk Determinations and Social Engineering

EDWARD ESCOBEDO
LEWIS UNIVERSITY
CPSC-59700 PROJECT PRESENTATION

Introduction

- Issue To Address
  - Social Engineering in Risk Assessments for the Navy
- Why Is this important
- Social Engineering Types
- Navy Security Control Assessors
  - Risk Management Framework
  - Security Categorization
  - Security Controls
- Variables to Consider
- Recommendation Solution



ISSUE: Risk Determinations for the Navy

- Navy Authorizing Authority (NAO) Tasking:
  - Assessors address Social Engineering
  - No general guidance exists
  - How much weight is should assessor consider

Social Engineering: Why is it Important

- Most common attack
- Gain information to penetrate networks and systems
- No technical skill is necessary
- Easiest attack due to human factor.

Ref: Schmittling, R. (n.d.). Performing a Security Risk Assessment. Retrieved May 7, 2017, from https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx

Social Engineering

- Navy's Biggest Issues
  - Phishing – 62%
  - Whaling – 22%
  - Vishing – 20%
  - Spim -25%

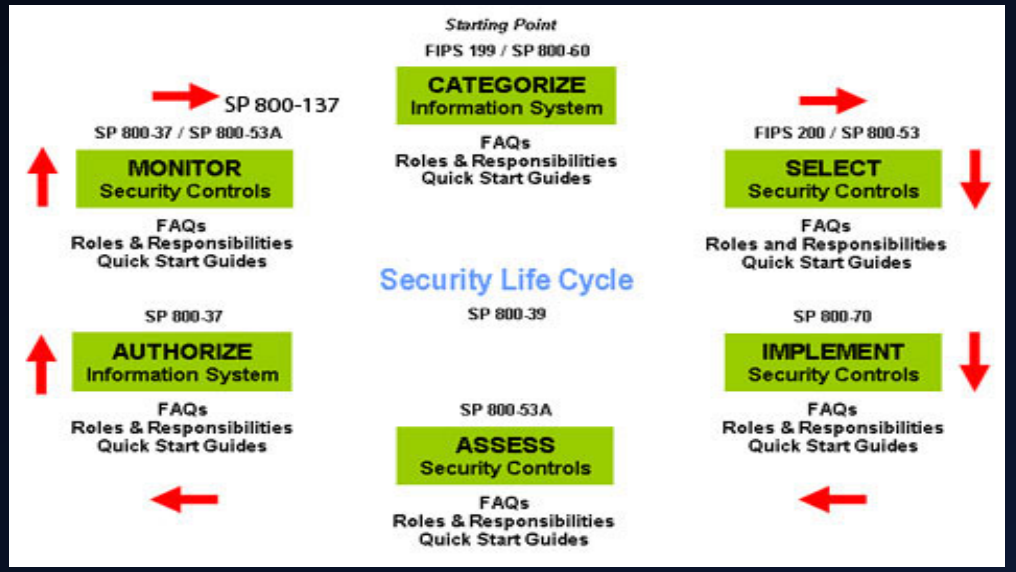
Ref: Courtney, W. B. (2014, April 28). The Social Engineering Infographic. Retrieved May 7, 2017, from https://new.social-engineer.org/social-engineering/social-engineering-infographic

Navy Security Control Assessor

- Risk Determinations for the Navy
  - 440 Ships / 1850 Shore Stations
- 14 Assessors
- Budget Cuts
  - 4 Hours per system

Navy Security Control Assessor

- Risk Management Framework
  - Repository for all system accreditations
- Program provide all Information
  - Certification and Accreditation plan
  - Architecture and data flow diagrams
  - Hardware/Software and Ports used
  - Risk Assessment Report and POA&M
- Risk Determination
  - High, Medium, Low



Ref: (2017, February 1). RISK MANAGEMENT FRAMEWORK (RMF). Retrieved May 7, 2017, from http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework

Security Controls

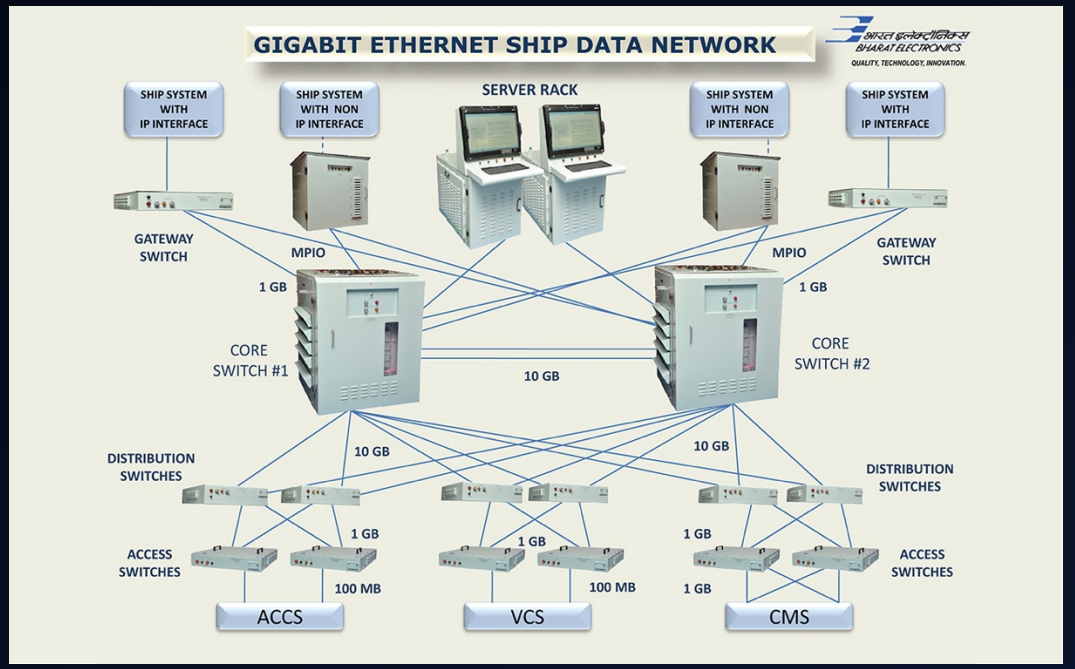
- 18 Family of controls
- Compliance
  - Scans needed to prove
- Social Engineering can cover multiple controls
  - How to prove controls is complaint

Defined in FIPS 200: Security Control Families and Their Identifiers			
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Certification, Accreditation, and Security Assessments	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information integrity
MA	Maintenance		

F. (2015, June). Cybersecurity Assessment Tool. Retrieved from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT

Variables for Considerations

- Starting Point
  - Security Polices
- Security Awareness
  - Quarterly Training is Required
  - Most neglected step
- System Complexity
- Number of Users
  - Privileged accounts to regular accounts



Courtney, W. B. (2014, April 28). The Social Engineering Infographic. Retrieved May 7, 2017, from https://new.social-engineer.org/social-engineering/social-engineering-infographic

Solution/Recommended Checklist

- Checklist will address the social engineering issues
  - Will not be a separate assessment
- Risk Determination
  - Accompany original assessment
  - Based on Categorization
    - CIA Triad

Checklist

	Social Engineering Risk Checklist
Risk Factor	Variables
System Characteristics	• Understand purpose • Number of General User/Privileged Users • Is system public facing
Access Control	• Is PKI used • Dual Authentication • Biometrics

Checklist

Security Polices	• **Written set of Social engineering policies** • **Visitor Management** • **Internet usage policy** • **User ID and Password Policy** • **Mobile Technology Use**
Physical Security	
Data	• Hard and Soft Copy Materials
Applications	• Black and Whitelisting
Awareness and Training	• How often Security Training/Awareness conducted • How does program track compliance
Incident Response	• How does program track incidents • Reporting and Incident Response Procedures

Conclusion

- SCA tasked to address social engineering
- Easy exploit due to human factor
- Different types to address
- Navy Assessors personnel and number of systems
- Program provides all information
- Creation of a standard checklist

Questions

References

- [1] Schmittling, R. (n.d.). Performing a Security Risk Assessment. Retrieved May 7, 2017, from https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx

- [2] Allen, M. (2006, June). SOCIAL ENGINEERING A MEANS TO VIOLATE A COMPUTER SYSTEM. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

- [3] MERCY, M. (n.d.). An Introduction to Social Engineering. Retrieved May 7, 2017, from https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf

- [4] Courtney, W. B. (2014, April 28). The Social Engineering Infographic. Retrieved May 7, 2017, from https://new.social-engineer.org/social-engineering/social-engineering-infographic/

References

- [5] (2017, February 1). RISK MANAGEMENT FRAMEWORK (RMF). Retrieved May 7, 2017, from http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework
- [6] Osterloo, B. (2008, March). Managing Social Engineering Risk. Retrieved May 7, 2017, from http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf
- [7] N. (n.d.). NIST Special Publication 800-53 (Rev. 4). Retrieved May 8, 2017, from https://nvd.nist.gov/800-53/Rev4/
- [8] Fu, P. L. (1997, November). Design Methodology for System Correctness. Retrieved from http://www.hpl.hp.com/techreports/tandem/TR-87.7.pdf
- [9] F. (2015, June). Cybersecurity Assessment Tool. Retrieved from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf