INFORMATION SECURITY

A DAY IN THE LIFE
WHO AM I?

• Security officer for MIE
• CISSP, CISA, CGEIT, CRISC, CRMA, PMP, FLMI and studying for CISM
• RMR and JA

• Interactive session – share stories
THREAT SOURCES

- Nation States
- Terrorists
- Industrial Spies
- Organized Crime
- Hacktivists
- Hackers
- Business Competitors
- Employees – accidental or deliberate

https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

https://hitrustalliance.net/threat-catalogue/
IT STARTS WITH THE DATA
BUSINESS ALIGNMENT

Mission of the Business

Strategic Business Objectives

Information Security

Mission: Develop, execute and maintain a proactive, company-wide security program based on strategic business objectives

Vision: Incorporate a continuous security mindset into all aspects of our business functions
GOVERNANCE

Board of Directors
IT Audit Committee
Policies
Standards
Procedures
Security Team
Compliance Team

InfoSec Objectives
OWNERSHIP

Data Owner
Asset Inventory
Data Classification

Governance
InfoSec Objectives
BUSINESS RESILIENCY

BCP
DRP
IRP
BIA

Ownership
Governance
InfoSec Objectives
_____ MANAGEMENT

Risk Analysis and Management
Patch Management
Vulnerability Management
Vendor/Supply Chain Management

https://www.google.com/alerts#

https://www.nist.gov/
https://csrc.nist.gov/
https://csrc.nist.gov/publications/detail/sp/800-161/final
TECHNICAL CONTROLS

AV
IDS/IPS
Encryption
Logging and Monitoring
DLP

Management
Resiliency
Ownership
Governance
InfoSec Objectives
STORY TIME

- Cost of a laptop is $2,000
- Additional cost of losing the laptop is $8,000
- Asset Value (AV) = $10,000
- Exposure Factor (EF) = 100%
- Single Lose Expectancy = $10,000
- On average, we “lose” 3 laptops per year (ARO)
- Annual Loss Expectancy (ALE) is $30,000
RETURN ON SECURITY INVESTMENT

ALE before encryption control        $30,000

Encryption cuts EF to 20%

ALE after implementing control       $6,000

+ Yearly cost of control             $20,000

Return on Security Investment        $4,000
3rd Party Assessments

External Pen Test
Internal Pen Test
Wireless Pen Test
Social Engineering

Controls
Management
Resiliency
Ownership
Governance
InfoSec Objectives
ACCESS CONTROL

Logical
Physical
Remote

3rd Party Assessments
Controls
Management
Resiliency
Ownership
Governance
InfoSec Objectives
KERBEROS
COMPLIANCE

HIPAA / HITECH
FISMA
FFIEC
GLBA
SOX
GDPR, CONSENT, CCPA, PIPEDA
Privacy Shield

Access Control
3rd Party Assessments
Controls
Management
Resiliency
Ownership
Governance
InfoSec Objectives
CERTIFICATIONS

SOC
HITRUST CSF
PCI – DSS
FedRAMP
Cloud Security Alliance
SECURITY AWARENESS

New hire training
Annual refresher training
Monthly newsletters
NCSAM – October
Periodic newsflashes

Compliance and Certifications
Access Control
3rd Party Assessments
Controls
Management
Resiliency
Ownership
Governance
InfoSec Objectives
DATA RECOVERABILITY

Online failover replica
Real-time replica offsite
Long-term offline backup
... STILL MORE

Cyber Insurance
Internal & External Audits
Regular exclusion checks:
OIG LEIE and SAM

https://oig.hhs.gov/exclusions/index.asp
https://www.sam.gov/SAM/
INFOSEC RECAP

• Not one person or a team of people; the entire organization
• Defense in depth
• If you see something, say something

• [https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity](https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity)