Balancing Compliance and Operational Security Demands

Nov 2015

Steve Winterfeld

What is more important?

- Compliance with laws / regulations
- Following industry best practices
- Developing a operational practice

The most important issue is getting the senior leadership to support your vision

Fire Marshal vs Firefighters

Federal – Government Focused

- Federal Information Security Management Act (FISMA) [Law]
- Risk Management Framework (RMF) for Department of Defense Information Technology (IT) [DoD cyber]
- Intelligence Community Directive (ICD) 503 [IC cyber]
- Federal Risk and Authorization Management Program [Cloud]
- North American Electric Reliability Corporation (NERC) [Energy]
- General Services Administration (GSA) / Office of Management and Budget (OMB) [Gov cyber]
- National Institute of Standards and Technology (NIST) [Guide]
- Executive Order on Cybersecurity / Presidential Policy Directive on Critical Infrastructure Security and Resilience [Framework]

Federal Financial Institutions Examination Council Cybersecurity Assessment Tool

- The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time
- Assessment is in two parts:
- Risk -

Category: Technologies and Connections	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)

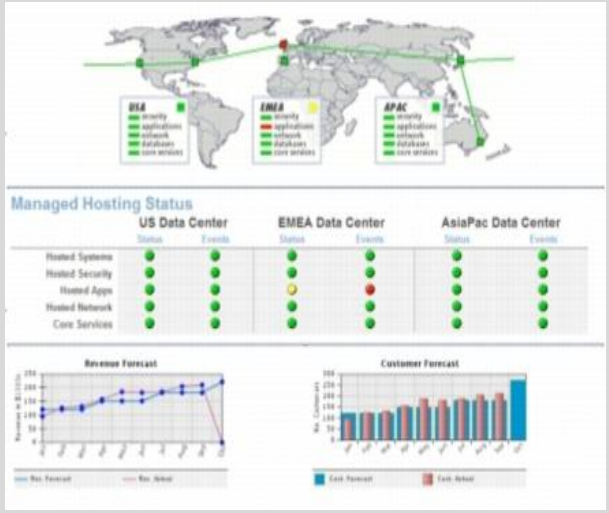
- Controls -

Maturity Levels
Innovative
Advanced
Intermediate
Evolving
Baseline

Federal - Commercial Focused

- Medical
  - Health Insurance Portability and Accountability Act (HIPAA)
- Business
  - Payment Card Industry (PCI) [credit cards]
  - Gramm Leach Bliley Act (GLBA) [financial institutions]
  - Sarbanes Oxley Act (SOX) [public companies]
  - Statement on Standards for Attestation Engagements (SSAE) 16
  - Service Organization Control (SOC)1 / 2 / 3

Motivations



Standards - Policies / Process / Audit

- Control Objectives for Information and related Technology (COBIT) by ISACA
- Factor Analysis of Information Risk (FAIR)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) by CMU CERT
- ADversary VIew Security Evaluation (ADVISE) by CMU CyLab
- Information Assurance Technical Framework (IATF)
- GTAG 15: Information Security Governance

Standards continued

- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)
- IT Infrastructure Library (ITIL) [IT focused, light on security]
- Six Sigma [cost efficiencies]
- Capability Maturity Model Integration (CMMI) [process]

GRC

- Governance
  - Policy / Controls (ie IDM)
  - Vendors (connections)
- Risk
  - Risk Appetite
- Compliance
  - Law / Regulation
  - Industry Standard
  - General Framework / Standard

Three layers of defense

- The First Line of Defense: Line Management
- The Second Line of Defense: Functional / Support Management
  - InfoSec
    - Compliance
    - Risk Register / Radar
    - Self Identified
- The Third Line of Defense: Internal Audit

Adjacent Functions and Focus Areas

- Audit
- Privacy
- Fraud
- Loss Prevention
- Physical Security
- eDiscovery
- Threat Intelligence
- Insider Threats
- Remediation
- Mergers and Acquisitions (M&A)

DevOps

- Change Control
  - Documentation
  - Testing
- Security
  - Peer review
- Separation of Duties
  - Two person dev teams

Identity Management / Access reviews

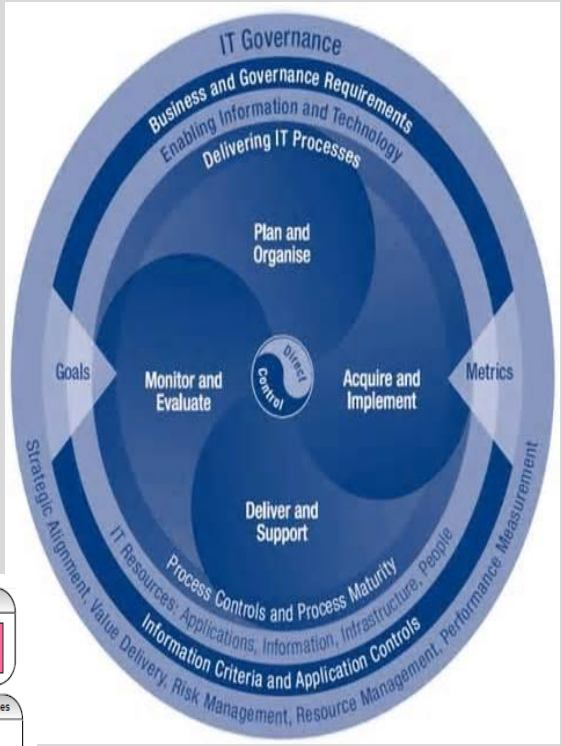
- Quarterly Access Reviews
- Automation
- Manager engagement
- HR engagement
- Network and Application security
- Tracking transfers within company
- Network vs Application access

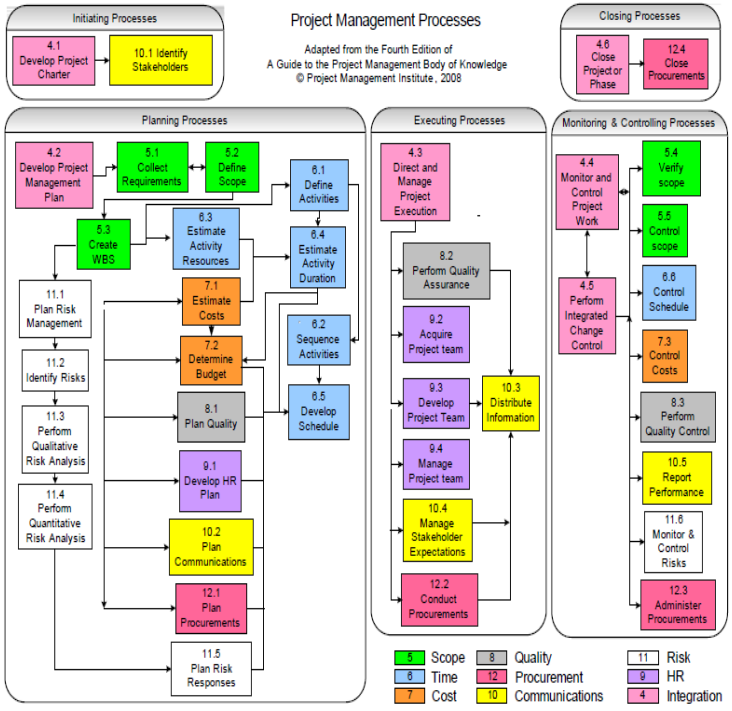
Major Event Incident Response (Breach)

- Plan – Prepare, Detect (pre internal, external not public, external public), Respond (contain and remove), Recover (remediate)
- Roles – Leadership, CIO, CISO, Privacy Officer, Legal, Human Resources, Privacy, Risk and Audit
- Contracted external support – PR, Forensics, Legal
- Determine triggers and thresholds
- Communications and use of Attorney Client Privilege
- Exercise

Techniques


Continual Process Improvement
Service Level Management
Service Catalogue Management
Availability Management
Supplier Management
Service Design
Configuration Management
System
Incident Management
ITIL
Service Strategy
Service Operation
Service Transition
Service Testing & Validation
Release & Deployment Management
Event Management
Problem Management
Change Management
Knowledge Management
Service Reporting and Service Measurement


IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Goals
Monitor and Evaluate
Direct
Control
Acquire and Implement
Metrics
Deliver and Support
Process Controls and Process Maturity
IT Resources- Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement


Project Management Processes
Adapted from the Fourth Edition of
A Guide to the Project Management Body of Knowledge
© Project Management Institute, 2008
Initiating Processes
4.1 Develop Project Charter
10.1 Identify Stakeholders
Closing Processes
4.6 Close Project or Phase
12.4 Close Procurements
Planning Processes
4.2 Develop Project Management Plan
5.1 Collect Requirements
5.2 Define Scope
6.1 Define Activities
5.3 Create WBS
6.3 Estimate Activity Resources
6.4 Estimate Activity Duration
11.1 Plan Risk Management
7.1 Estimate Costs
6.2 Sequence Activities
11.2 Identify Risks
7.2 Determine Budget
11.3 Perform Qualitative Risk Analysis
8.1 Plan Quality
6.5 Develop Schedule
11.4 Perform Quantitative Risk Analysis
9.1 Develop HR Plan
10.2 Plan Communications
12.1 Plan Procurements
11.5 Plan Risk Responses
Executing Processes
4.3 Direct and Manage Project Execution
8.2 Perform Quality Assurance
9.2 Acquire Project team
9.3 Develop Project Team
10.3 Distribute Information
9.4 Manage Project team
10.4 Manage Stakeholder Expectations
12.2 Conduct Procurements
Monitoring & Controlling Processes
4.4 Monitor and Control Project Work
5.4 Verify scope
5.5 Control scope
4.5 Perform Integrated Change Control
6.6 Control Schedule
7.3 Control Costs
8.3 Perform Quality Control
10.5 Report Performance
11.6 Monitor & Control Risks
12.3 Administer Procurements
5 Scope
6 Time
7 Cost
8 Quality
12 Procurement
10 Communications
11 Risk
9 HR
4 Integration

Key Components of a Program

- Programmatics
  - Strategy (Business, IT and Security)
  - Threat profile
  - Risk profile
  - Special req like 10K cyber statements
  - Metrics / Visualization

Program Drivers

- Impacts analysis
  - Loss of Intellectual Property (IP)
  - Loss to brand reputation
  - Legal (fines / law suits)
- Impact of Legislation
  - New reg or laws like PCI 3.1, NERC CIP 5 or NIST Security Framework

Management Drivers

- Organizational structure
  - Review effectiveness and efficiencies of Information Security Organization Policies and Procedures
  - Security monitoring and incident response plan
  - Investigations (forensics and e-discovery)
  - Business Continuity Plan / Disaster Recovery Plan
  - For companies developing software – software assurance process and tools

Leadership Drivers

- Organization issues
  - Relationship between compliance, audit, privacy, fraud, security (physical and cyber) and business needs
  - Culture of the organization
  - Vulnerability Assessment & Penetration Test program
  - Access management program
  - Mobile device protection program
  - Social Media management program
  - Supply line issues identification

Who we are talking to determines what we talk about

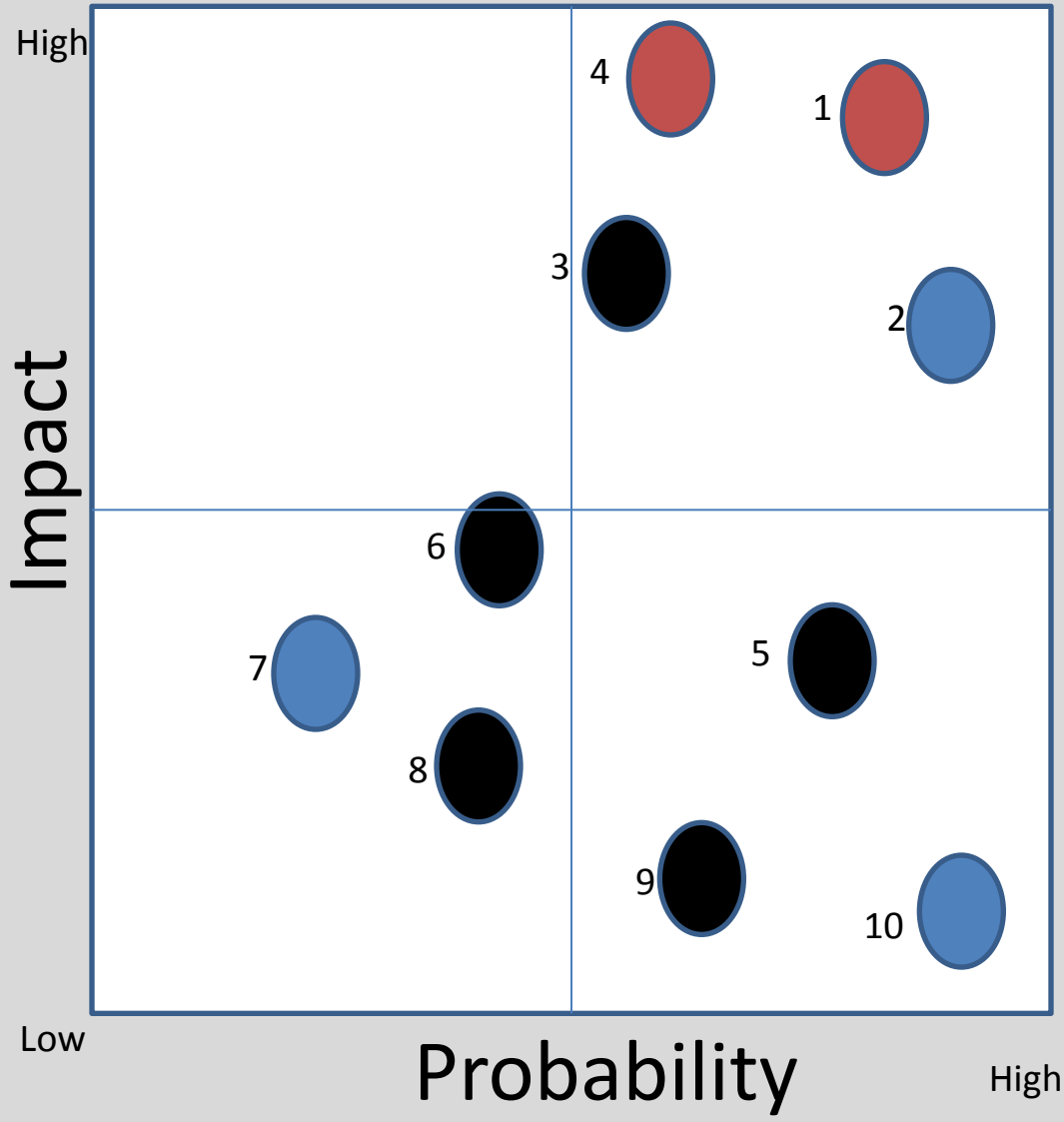
Tying it together

- Risk Radar / Register
  - Risk Control based
- Talk to resources and impacts

Ensure leadership is equipped to make decisions about accepting risk

Sample Risk Radar

(based on control weakness)



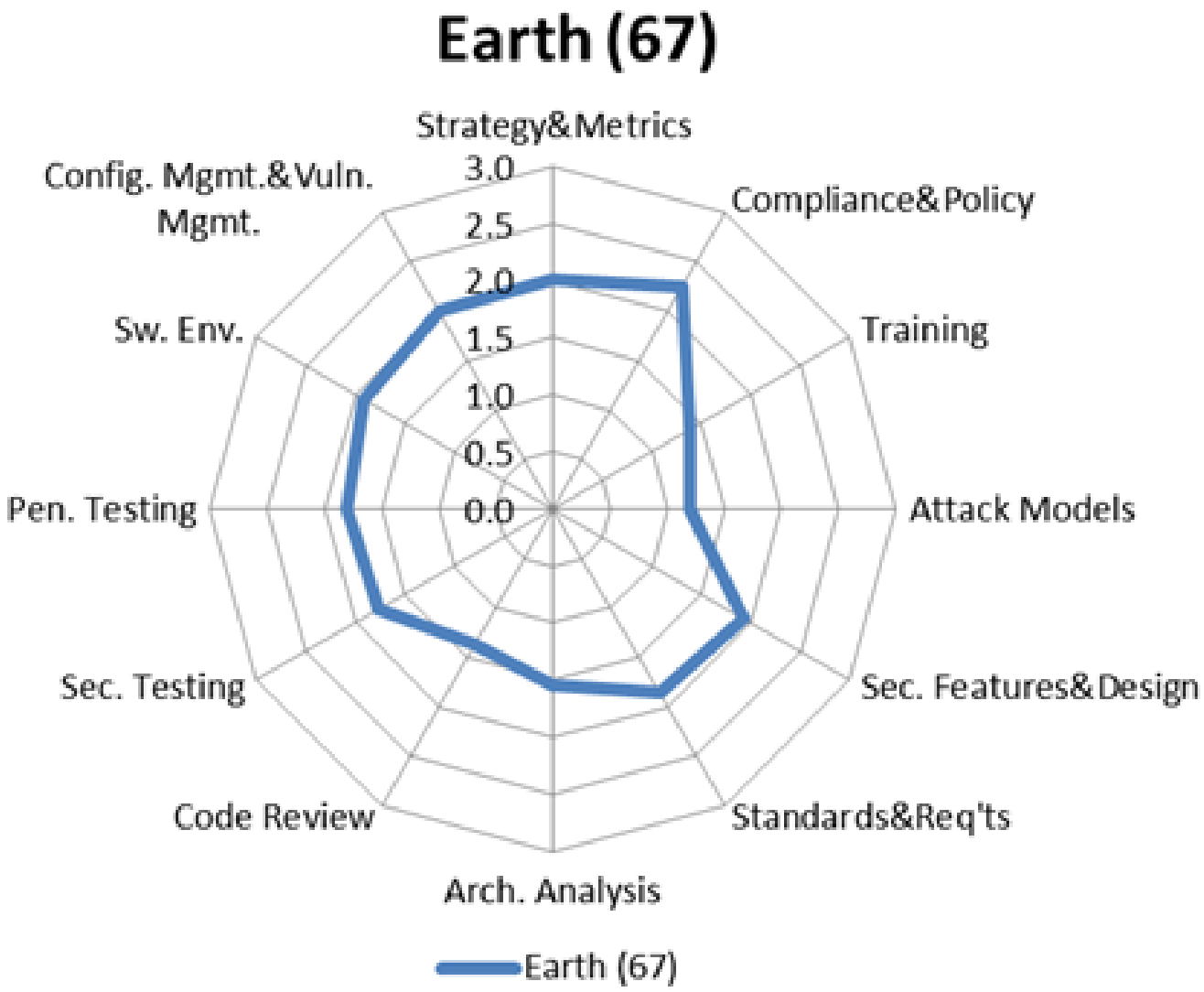
Control
1. Compliance
2. Training
3. Asset Man
4. SOC
5. Upgrade FW
6. Insider Threat
7. Policy Dev
8. Encryption
9. BC/DR
10. Pen Testing

Under $50K

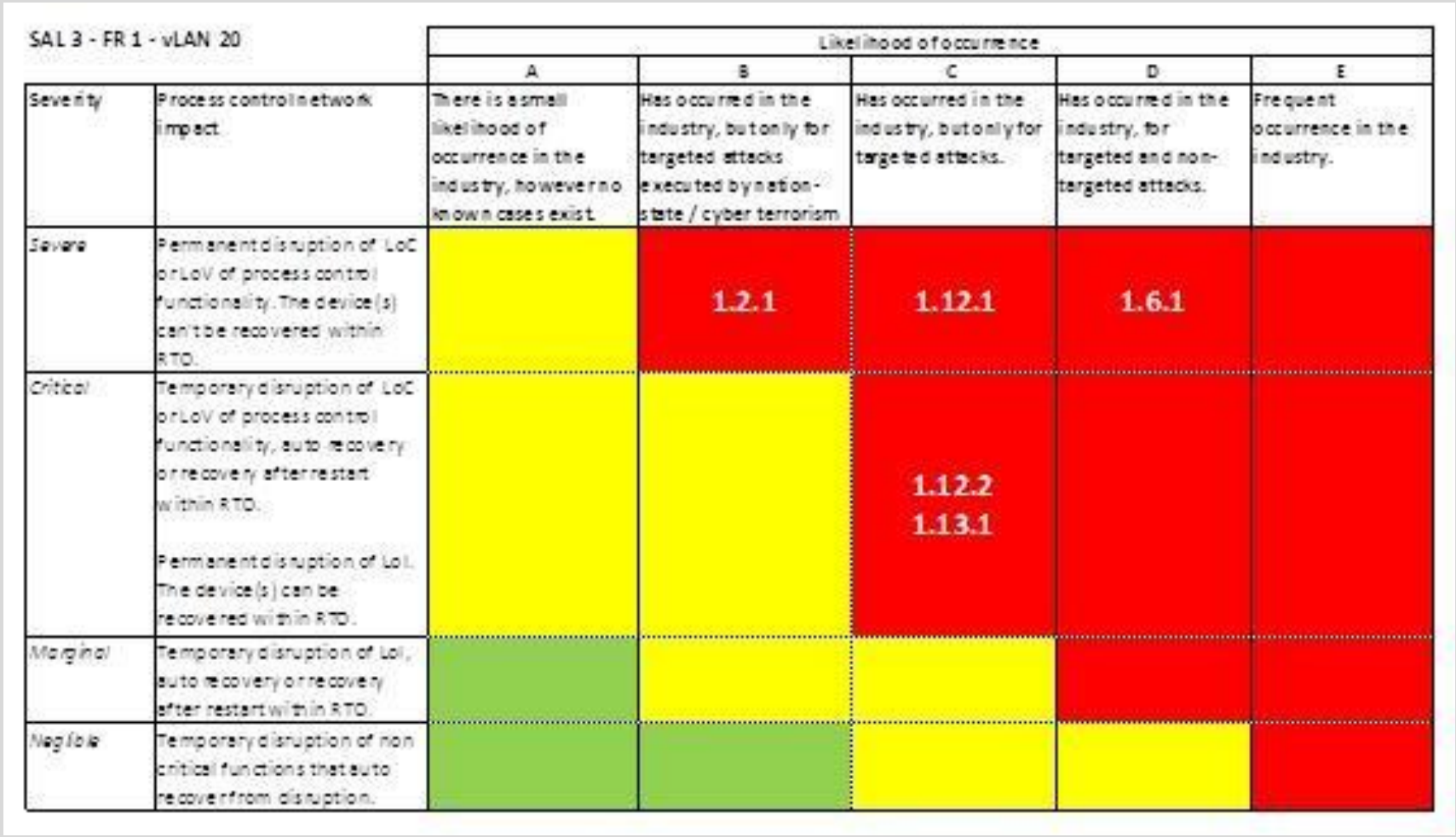
$50K to $500K

Over $500K

Spider Chart



Heat Map / Probability Chart



SAL 3 - FR 1 - vLAN 20		Likelihood of occurrence				
		A	B	C	D	E
Severity	Process control network impact	There is a small likelihood of occurrence in the industry, however no known cases exist.	Has occurred in the industry, but only for targeted attacks executed by nation-state / cyber terrorism	Has occurred in the industry, but only for targeted attacks.	Has occurred in the industry, for targeted and non-targeted attacks.	Frequent occurrence in the industry.
Severe	Permanent disruption of LoC or LoV of process control functionality. The device(s) can be recovered within RTO.		1.2.1	1.12.1	1.6.1	
Critical	Temporary disruption of LoC or LoV of process control functionality, auto recovery or recovery after restart within RTO. Permanent disruption of LoI. The device(s) can be recovered within RTO.			1.12.2 1.13.1		
Marginal	Temporary disruption of LoI, auto recovery or recovery after restart within RTO.					
Negligible	Temporary disruption of non critical functions that auto recover from disruption.					

What's next

- Your job is to make sure leadership understands the risks and are equipped to make decision on where to accept it
- Build consensus on criteria, definition, impact ranking and visualization of risk.
- Implement a plan based on return on impact of risk mitigation

Questions

= 42

THE CYBER THREAT LANDSCAPE

THREATS

ATTACK METHODOLOGY

RECON
- SCANNERS
- SNIFFERS
- PACKET CRAFTERS

ATTACK
- EXPLOIT VULNERABILITIES
- COMPROMISE APPLICATIONS
- CRACK PASSWORDS

EXPLOIT
- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY

SOCIAL ENGINEERING
- VIA TECHNOLOGY
- VIA HUMAN

TOOLS AND TECHNIQUES
- ROOTKIT
- NESSUS
- WEB ATTACKS
- TROJAN HORSE
- BOTNETS
- PHYSICAL THREAT
- WORMS
- ZOMBIES
- METASPLOIT
- VIRUSES
- SOCIAL NETWORKS
- SQL ATTACK
- PHISHING
- BACKDOORS
- PHARMING
- SPEAR PHISHING
- WIRELESS
- MOBILE
- CROSS-SITE SCRIPTING
- DISTRIBUTED DENIAL OF SERVICE (DDOS)
- CAIN & ABEL
- WIRESHARK
- BUFFER OVEFLOW
- SPAM
- DATABASE ATTACKS

ATTACKERS

CYBER WARFARE

ADVANCED PERSISTENT THREAT (APT)
- CHINA
- DIGITAL SPYING
- RUSSIA
- ESPIONAGE

ORGANIZED CRIME
- NIGERIAN SCAMS
- RUSSIAN BUSINESS NETWORK
- PHISHING
- CUSTOM BANK ATTACKS

INSIDERS
- DISGRUNTLED
- FINANCIALLY MOTIVATED
- UNINTENTIONAL

HACKTIVISM
- POLITICAL
- RELIGIOUS
- CULTURIAL
- NATIONAL PRIDE
- TERRORIST
- SOCIAL HACKING
- GROUP MEMBERSHIP

SCRIPT KIDDIES (NOOBS)
- CHALLENGE
- STATUS
- CURIOSITY
- ENTERTAINMENT

DEFENSIVE MOUNTAIN RANGE

DEFENSE-IN-DEPTH TOOLS
- ENCRYPTION
- INTRUSION DETECTION SYSTEM
- FIREWALLS
- ANTI-VIRUS
- METRICS

SECURITY OPERATIONS CENTER
- INCIDENT RESPONSE TEAM
- VULNERABILITY ASSESSMENTS
- PENETRATION TESTS
- FORENSICS

CONFIGURATION MANAGEMENT
- PATCHING
- POLICIES
- ACCESS CONTROL

IDENTITY MANAGEMENT
- AUTHENTICATE
- AUTHORIZE
- AUDIT (PDI/PCI/SOX/GLB)

RISK MANAGEMENT
- SITUATIONAL AWARENESS
- DISASTER RECOVERY
- CONTINUITY OF OPERATIONS
- DUE CARE / DILLIGENCE
- ANNUALIZED LOSS EXPECTANCY

KEY EDUCATION TECHNIQUES
- TRAINING
  - ·LEADERS
  - ·SYSTEM ADMINS
  - ·USERS
  - ·SECURITY
- HONEYPOTS
- VIRTUAL
  - ·MACHINES
  - ·WORLDS
- KNOPPIX

TARGETED CAPABILITIES
- BANKING
- MILITARY
- LAWS
- HEALTH
- LAW ENFORCEMENT
- TRANSFORMATION

NATIONAL CRITICAL INFRASTRUCTURE
- AVIATION
- CHEMICAL
- ENERGY
- MANUFACTURING
- STATE
- COMMERCE
- EMERGENCY SERVICES

CORPORATE
- PLANS
- ORGANIZATION
- TRADE SECRET
- E-MAIL
- PROPRIETARY
- FINANCE
- PROPOSALS
- POLICY

FINANCE
- CREDIT CARD
- BANK
- CREDIT

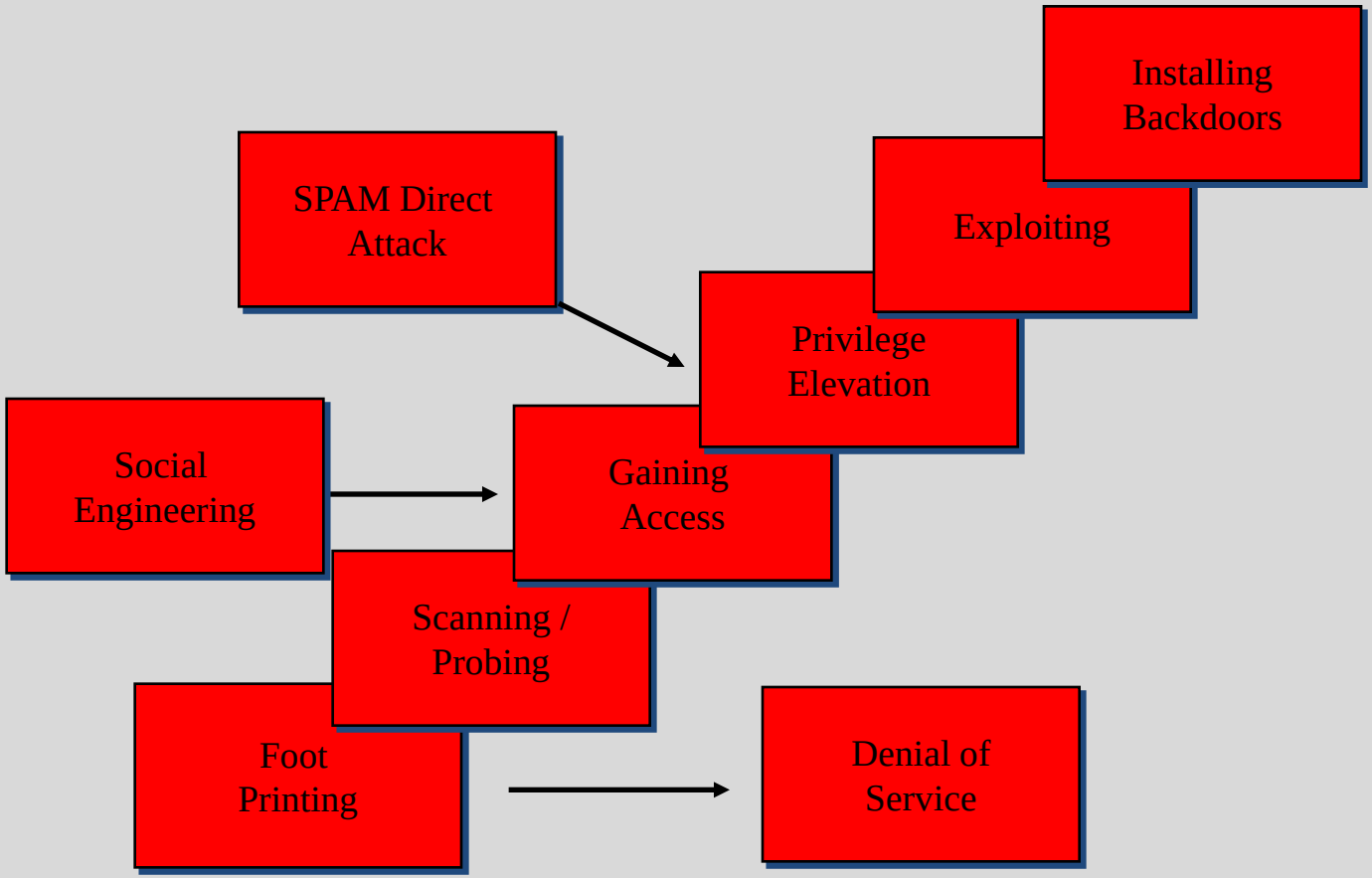
PERSONAL
- HEALTH
- SSN
- SOCIAL NETWORKS
- SPENDING HABITS
- WINDOWS

I.T. INFRASTRUCTURE
- VOIP
- CLOUD
- APPLICATIONS
- CONFIGURATION
- ARCHITECTURE
- CISCO
- WEB PAGES

iDEFENSE

TASC

Anatomy of an Attack



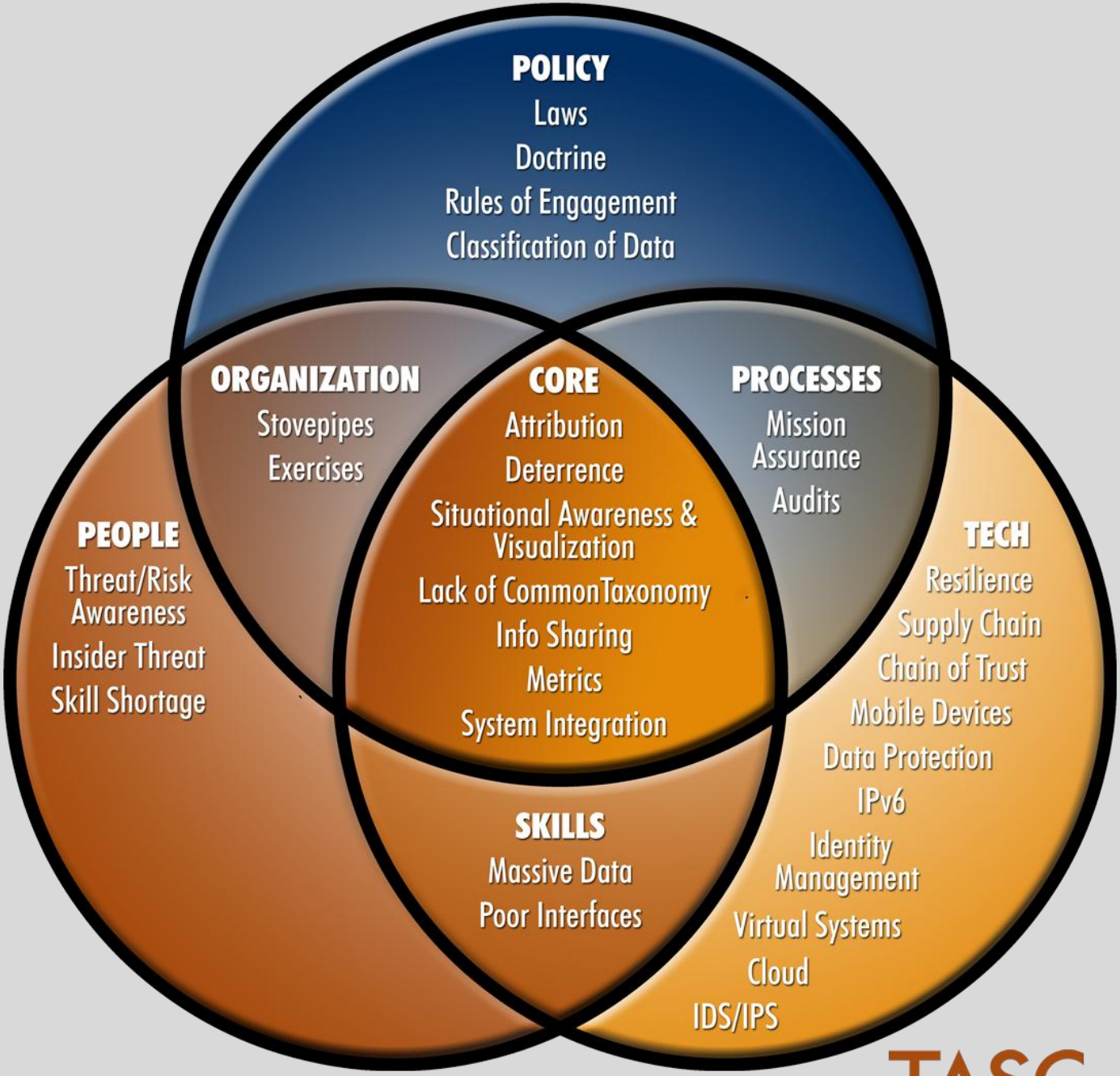
STOP. THINK. CONNECT.

STOP. Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK. Take a moment to be certain the path is clear ahead. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT. Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Visit http://www.stopthinkconnect.org for more tips on safety online.


POLICY
Laws
Doctrine
Rules of Engagement
Classification of Data
ORGANIZATION
Stovepipes
Exercises
CORE
Attribution
Deterrence
Situational Awareness & Visualization
Lack of CommonTaxonomy
Info Sharing
Metrics
System Integration
PROCESSES
Mission Assurance
Audits
PEOPLE
Threat/Risk Awareness
Insider Threat
Skill Shortage
SKILLS
Massive Data
Poor Interfaces
TECH
Resilience
Supply Chain
Chain of Trust
Mobile Devices
Data Protection
IPv6
Identity Management
Virtual Systems
Cloud
IDS/IPS

TASC