
McAfee
An Intel Company
Foundstone
Professional Services
Data Risk Assessment – DRA
Who's Watching Your Back?
Jeff Tucker – Principal Consultant
Jeff.Tucker@Foundstone.com
712.322.2200
SAFE NEVER SLEEPS.
Foundstone Professional Services

About the Presenter

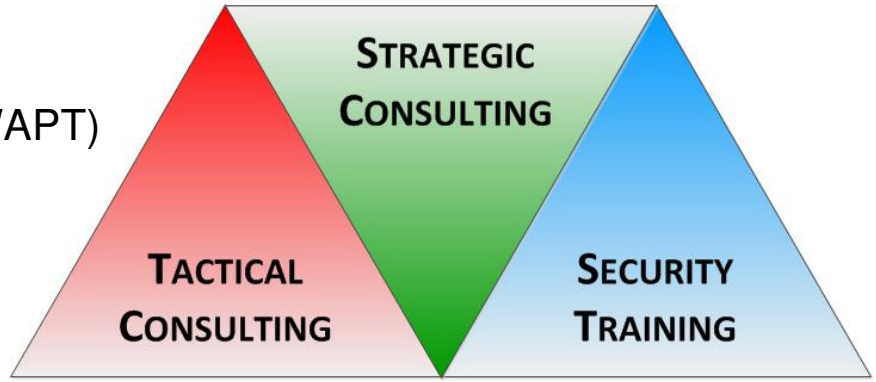
Jeff Tucker

- Principal Consultant, Foundstone Professional Services
- Federal Engagement Manager
- Bachelor of Science Degree – Computer Information Systems
- Master of Science Degree – Security Management
- PCI QSA, CISSP, CISA, MCSE
- Foundstone Service Line Lead (Strategic Services)
  - FISMA, PCI, GLBA (FFIEC), HIPAA
  - Security Control Assessments (SCAs)
  - Data Security Assessments
  - Risk Assessments
  - Security Program Development (Policies, Plans and Procedures)

Jeff.Tucker@Foundstone.com

Foundstone's Services

- Compliance and Risk Management
  - FISMA, PCI DSS, GLBA (FFIEC), HIPAA
  - Security Control Assessments (SCAs)
  - Data Security Assessments
- Risk Management
  - **Risk Assessments (systems, critical data, and the enterprise)**
  - Strategic and Tactical Security Assessments
  - Network and Security Architecture Analysis
  - Security Program Development
- Tactical Security Testing
  - Web Application Penetration Testing (WAPT)
  - Internal and External Network Testing
  - Social Engineering
- Security Training
  - DoD
  - Ultimate Hacking



Jeff.Tucker@Foundstone.com

Benefits of a Data Risk Assessment

1. Preserve Revenue
2. Align the allocation of recourses to the Needs of the Business
3. Risk-Based Security Program that aligns controls with risk levels
4. Determine Appropriate Security Requirements
5. Improved Planning
6. Justify or Control Spending Based on Risk Levels
7. Preempt Surprises
8. Find and Remediate Security Holes to improve security posture
9. Increase Motivation and Awareness
10. Document Due Diligence

Jeff.Tucker@Foundstone.com

What Is Risk? – Definitions

Definitions

Risk is the probability or potential of an event causing a negative impact (loss, harm or damage). An estimate of what might happen

Risk Factors –1) Threat, 2) Vulnerability, and 3) Impact.

Threat is a combination of 'Threat Source/Agent' and 'Threat Event' that may create any circumstance or event with the potential to adverse impact.

Vulnerability is a flaw, weakness, predisposing condition or circumstance.

Impact; in terms of security, is the adverse result of an event that causes loss or damage. In a DRA, impact is determined during the data classification process.

Jeff.Tucker@Foundstone.com

What Is a Risk Assessments

Risk Assessment is a process to determine the level of risk to something:

1. Country, State or City
2. Company Enterprise
3. Facility – research complex, processing center, etc.
4. Network of Computer Systems
5. Information System (e.g. 3 tiered web application – presentation layer, application , and database)
6. Single Computer
7. Critical or Regulated Data

The methodology presented here is based on NIST SP 800-30 and is aligned with ISO 27005.

Jeff.Tucker@Foundstone.com

Approach and Methods

Approach

Four phases that follow methods based on NIST SP 800-30, Guide for Conducting Risk Assessments.

Phase 1: Data Identification & Impact Analysis → **Phase 2: Threat Analysis** → **Phase 3: Vulnerability Analysis** → **Phase 4: Risks Determination**

Methods

- Hybrid Analysis (Qualitative and Quantitative)
- Interview key personnel
- Review documents, policies and procedures
- Review results from security tests
- Review Data Flows

Jeff.Tucker@Foundstone.com

Empirical Data

Approach

Get the Facts – Empirical Data

- Understand the Data Flow.
- Interview Key Personnel on operations and procedures
- Review Policies and Procedures
- Evaluate Tactical Security Test Results

Jeff.Tucker@Foundstone.com

Risk Determination

Analysis or detailed examination of the of the three factors or elements of risk.

Threats – Vulnerability – Impact to Asset (Data)

Risk Equation Variations:

- Risk = (Threat × (Flaws-Safeguards)) x Impact.
- Risk = (Likelihood of a successful threat event) x Impact (i.e. Degradation of Confidentiality, Integrity or Availability
- Risk = (Likelihood) x Data Security Classification

Likelihood is the overall likelihood (P1) of a successful threat event will result in adverse impact or loss.

Its derived from the product of the likelihood of a threat event's occurrence (i.e. Threat) and the likelihood of the threat event's success (i.e. Vulnerability).

Jeff.Tucker@Foundstone.com

Risk Determination

Risk Analysis

Estimate the likelihood; probability (P1) of the occurrence of an event that will adversely impact your data.

Hybrid Analysis (Qualitative and Quantitative)

$$P(a) = \left[\frac{\sum_{i=0}^{a-1} \binom{1-p}{p}^{i}}{\sum_{i=0}^{a+b-1} \binom{1-p}{p}^{i}} \right]$$

Analysis of the three factors used to determine risk;

1. Impact: Estimate Damage
2. Threat: Saturation of Threats (likelihood of event)
3. Vulnerability: Rate Flaws (likelihood of successful exploit)

Jeff.Tucker@Foundstone.com

Assessment Process

Analysis

1. **Impact** – Identify data and data systems, and determine its sensitivity or security classification, and assign a quantitative value; i.e. numeric score.
2. **Threats** – Determine the likelihood of an incident (threat event) by identifying threat sources, their saturation, motivation and capabilities, calculating frequency of event occurrences, and assigning a numeric score.
3. **Vulnerabilities** – Determine the likelihood of an attack's success by identifying vulnerabilities, rating their severity, and assigning a numeric score.

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Impact Analysis

- Security classifications based on the potential impact
- The security objectives or factors that determine data classification (CIA) hold different values for different organizations.
- Usually these three factors are not equal.
- In most cases, with the exception of SOX, regulatory concerns focus on confidentiality
- Use a high water mark to classify systems – I.e. all data (system configurations, etc.) has the same security classification as the most sensitive data processed, transmitted or stored in any system located in the network.

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Impact Analysis

- FIPS Security Classification

Qualitative	Quantitative	Description
H	3	**High**: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
M	2	**Moderate**: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
L	1	**Low**: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Impact Analysis

- Example Impact Analysis

Data Security Classification	Rating	Score
Confidentiality	H	5.75
Integrity	M	2.00
Availability	M	1.50
Data Security Classification	HIGH	3.00

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Threat Analysis

1. Types of Threat Agents/Sources
2. Motivation and Capabilities
3. Saturation of Threat Agents
4. Attack Vectors
5. Prevalence or Frequency of Attempted Attacks (Threat Events)

A Threat Event Occurrence is merely an attempt to compromise data security.

The Likelihood of Event Occurrence is a combination of the saturation of Threat Agents and the Frequency of Threat Events against the industry to which the assessed entity is a member.

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Types of Threat Agents

1. Cyber and Physical – Man and Nature
2. Internal and External
3. Trusted Insider
4. Intruder or Malicious Users (Adversary)
5. Employee Error
6. Advanced Persistent Threats (APTs)

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Threat Source	Description	Saturation of Threat Source	Threat Event	Industry Occurrences	Likelihood of Occurrence
Internal Cyber Threats					
Trusted Insider	Trusted employee or contractor that has some level of authorized privileged access, and has the intent and means to access sensitive information for personal gain.	**Low**	An authorized employee attempts to directly copy or take customer data and remove it from the control of the company. System administrator deliberately modifies system parameters with the intent of degrading security controls. An individual who has authorized low-level access to organizational information systems, but gains (or attempts to gain) elevated access that exceeds authorization.	**Low**	**Low**
Malicious internal user or adversary with intent and means to exploit vulnerabilities in information system components, processes or procedures that can only be attacked from within the organization.	Individuals, groups, organizations, or states that have the ability to attack from within (including those that have gained unauthorized access), and seek to exploit vulnerabilities in information system components, processes or procedures.	**Medium**	Adversary attempts to exploit discovered vulnerabilities.	**Medium**	**Medium**
Employee Error	Erroneous actions taken by individuals in the course of executing their everyday responsibilities. An employee may be a manager, DBA, system administrator, network engineer, user or other employee	**Low**	Misconfiguration of systems. Authorized privileged user inadvertently exposes critical/sensitive information. Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a sensitivity or security classification which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.	**Medium**	**Medium**
				Estimated Likelihood of an Internal Cyber Threat Occurrence	**Medium**

Risk Assessment Process

Threat Source	Description	Saturation of Threat Source	Threat Event	Industry Occurrences	Likelihood of Occurrence
External Cyber Threats					
Malicious adversary with intent and means to exploit vulnerabilities in information system components that can be attacked remotely from outside of the organization's boundaries.	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.	**High**	Adversary launches a cyber attack targeting vulnerabilities in public-facing systems.	**High**	**High**
Malicious adversary with intent and means to initiate phishing and spear phishing attacks.	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.	**High**	End user messaging systems (email, etc.) receive fraudulent emails designed to gain unauthorized confidential and financial information.	**Medium**	**High**
Malicious code; e.g. worm, virus, Trojan Horse, etc.	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.	**High**	Adversary attempts to insert malware or otherwise corrupts critical internal organizational information systems.	**High**	**High**
Malicious adversary with intent and means to initiate denial of service attacks.	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.	**High**	Adversary launches attacks specifically intended to impede the ability of organizations to function.	**Medium**	**High**
				Estimated Likelihood of an External Cyber Threat Occurrence	**High**

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Threat Source	Description	Prevalence of Threat Source	Threat Event	Industry Occurrences	Likelihood of Event Occurrence
Physical Threats					
Malicious employees with intent and means to initiate attacks against physical assets located in the workplace.	Individuals, groups, organizations, or states that seek to exploit physical access controls.	**Low**	Theft of computers, storage media, files, etc.	**Medium**	**Medium**
Malicious Persons with intent and means to initiate attacks against physical assets located at facilities.	Individuals, groups, organizations, or states that seek to exploit physical access controls.	**High**	Theft of computers, storage media, files, etc.	**Medium**	**High**
Malicious Persons with intent and means to initiate attacks of opportunity against physical assets located in cards, hotels, restaurants, homes, etc..	Individuals, groups, organizations, or states that seek to exploit physical access controls.	**Medium**	Theft of computers, storage media, files, etc.	**Low**	**Medium**
				Estimated Likelihood of an External Cyber Threat Occurrence	**Medium**

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Threat Ratings	Score	Rating
Estimated Likelihood of an Internal Cyber Threat Occurrence	2.08	**Medium**
Estimated Likelihood of an External Cyber Threat Occurrence	3.44	**High**
Estimated Likelihood of an External Cyber Threat Occurrence	**3.45**	**HIGH**
Estimated Likelihood of a Physical Threat Occurrence	**2.29**	**Medium**

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Vulnerability Analysis

Focus on security controls and processes (NIST, ISO, PCI)

- Required Data Security Controls
- Established Security Policies and Procedures
- Maintained Security Processes

Assess these areas

- Information Security Governance
- Data Risk Management Practices
- Secure Data Operations/Handling.
- Information Security Program.

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Governance Processes

- Security Governance Committee
  - Charter Established and Clearly Defined Goals.
  - Committee Is Inclusive
- Committee Responsibilities
  - Review and approves security policies?
  - Align Security with Business Needs.
  - Risk Assessments Guide Security Investments.
- Assigned Security Responsibilities
  - Chief Information Security Officer
  - Incident Response
  - Independent Audits
  - Security Awareness Program
  - Service Provider Management

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Data Risk Management

- Data Ownership and Responsibilities
- Data Identification and Classification (Inventory)
- Segmented Data Processing and Storage Networks
- Data Access Authorization Process
  - Limits Access Based on Need and Least Privilege
- Periodic Risk Assessments
  - Data Owners Review Assessment Reports.
  - Security Policies Are Reviewed Annually and Updated as Needed
- Risk Treatment and Acceptance
  - Treatment and Acceptance Criteria
  - Acceptance Requires Data Owner's Authorization

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Secure Data Operations/Handling

- Secure Procedures
  - Support the Policies and Facilitate Data Security.
  - Have been Implemented.
  - Reviewed and Updated as Needed
  - Include Effective Safeguards
- Security Awareness Training
  - Security Policies and Procedures.
  - Aware of the Classification
  - Job Specific Training

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Information Security Program.

Security Processes

1. Build and Maintain Secure Networks
2. Data Protection Requirement (at rest and in transit)
3. Vulnerability Management Programs/Process
4. Monitoring
   (Security Event Information Analysis)
5. Periodic Security Testing
6. Publish, Disseminate and Maintain
   Security Policies, Plans, and Procedures

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Vulnerability Analysis

Vulnerability score based on Implementation of Security Controls
(i.e. Safeguards / Counter Measures)

- Maximum Vulnerability Score = Raw Vulnerability
  Effort x Threat Vector x Degradation (Impact)
- Effectiveness of Control x Implementation Status
  - In Place = 0
  - Substantially In Place = .33
  - Partially In Place = .75
  - Not In Place = 1

Vulnerability Score =
(Maximum Score) x (Implementation Status) I.e. Vulnerability – Safeguards

Jeff.Tucker@Foundstone.com

Risk Assessment Process

Vulnerability Analysis

Additional Safeguards:

1. Cryptography and Tokenization
2. Network Segmentation with Strong Access Controls
3. Data Boundaries
4. Leakage Monitoring (DLP)

Jeff.Tucker@Foundstone.com

How Secure Is Your Data

Calculating Risk

- Vulnerability x Threat = Likelihood
- Likelihood x Data Classification = Risk

Data Risk Management Category	Vulnerability	Threat	Likelihood	Data Classification	Risk Score	Risk Rating
Security Governance	**0.7**	**1.44**	**0.99**	**2.67**	**2.64**	**LOW**
Security Governance Committee	**0.7**	**1.00**	**0.67**	**2.67**	**1.79**	**LOW**
Committee Responsibilities	**0.5**	**1.00**	**0.46**	**2.67**	**1.22**	**LOW**
Assignment of Security Responsibilities	**0.2**	**1.88**	**0.29**	**2.67**	**0.76**	**NEGLIGIBLE**
Security Plans	**0.9**	**1.88**	**1.72**	**2.67**	**4.58**	**MEDIUM**

Jeff.Tucker@Foundstone.com

How Secure Is Your Data

Estimated Risk

Risk Control Category	Score	Rating
Overall Ratings	**11.97**	**MEDIUM**
Security Governance	3.50	**LOW**
Data Risk Management	9.36	**MEDIUM**
Data Operations	4.67	**MEDIUM**
Information Security Program	19.83	**HIGH**

Jeff.Tucker@Foundstone.com

Conclusion

1. Data Centric Assessment
2. Understand the Data Flows
3. Hybrid Analysis of Threats, Vulnerabilities and Impact
4. Collect Empirical Data (Get the Facts)
5. Include Tactical Security Assessments

Risk Is an Estimate of what Might Happen!

Jeff.Tucker@Foundstone.com

Questions

Jeff.Tucker@Foundstone.com

Foundstone Professional Services

Jeff Tucker – Principal Consultant

Jeff.Tucker@Foundstone.com

712.322.2200