SECURITY RISK MANAGEMENT

ISACA Atlanta Chapter, Geek Week

August 20, 2013

Scott Ritchie, Manager, HA&W Information Assurance Services

Scott Ritchie
CISSP, CISA, PCI QSA, ISO 27001 Auditor

- Manager, HA&W Information Assurance Services
- Previous
  - AT&T, Internal Audit (Technology audits)
  - Scientific Research Corp., Information Systems Security Officer
- Academics
  - M.B.A.
  - M.S. Information Assurance

Scott.Ritchie@hawcpa.com
(770) 353-2761

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

HA&W Information Assurance Services

Key Verticals:	SME Domains:	Key Services:
❑ Fraud & Analytics ❑ Healthcare IT ❑ Tech / Cloud Service Providers ❑ FinTech / Payments	➢ Security ➢ Privacy: o HIPAA / HITECH o Safe Harbor o State Regulations ➢ Confidentiality ➢ Processing Integrity ➢ Data Management ➢ Availability ➢ Financial Reporting	• Risk and gap assessments • Attest/Compliance Reporting: • SSAE 16 & SOC 2 Reporting • PCI Compliance • ISO 27001 Certification • FedRAMP Certification • IT Internal Audit • IT Governance • Due Diligence

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Focus of Today's Presentation

- How to assess security risks
- Understand recognized security risk management frameworks
- Introduce security risk management practices

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Security Environment

- Explosive growth/ aggressive use of technology
- Proliferation of data
- Sophistication of threats

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Challenges

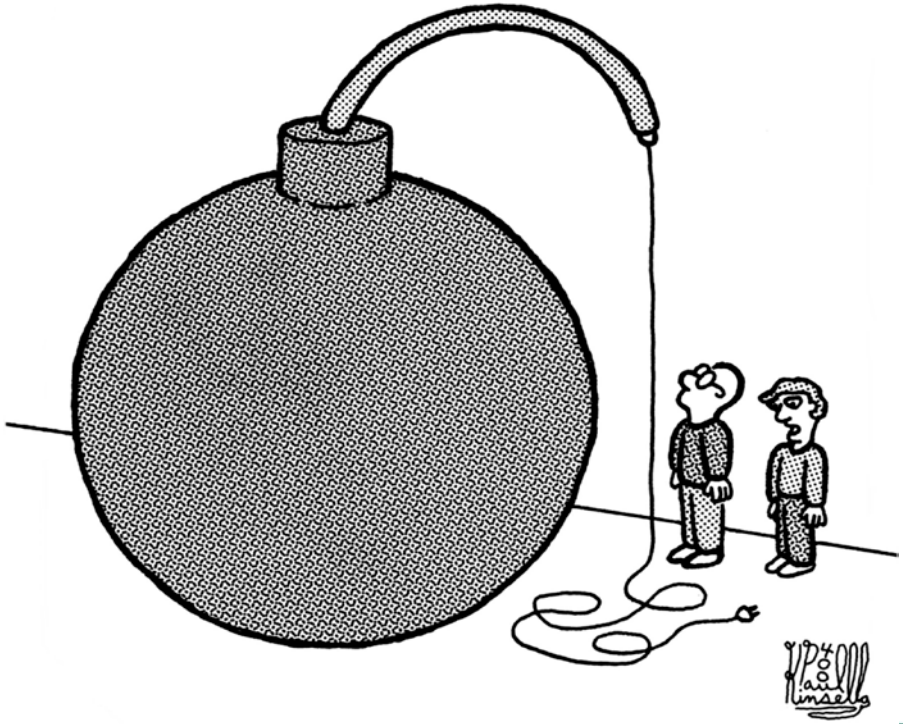
- **Least privilege**
- Awareness and **training**
- Insider threat
- Advanced Persistent Threats
- Trustworthiness of applications and systems
- Mobile computing
- Cloud and virtualization
- Individual/device auth
- **Resiliency** of Systems
- Privacy
- **Supply chain**

Can't cover everything - Risk management allows prioritization

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk Assessment Illustrated



"I don't think we should plug it in."

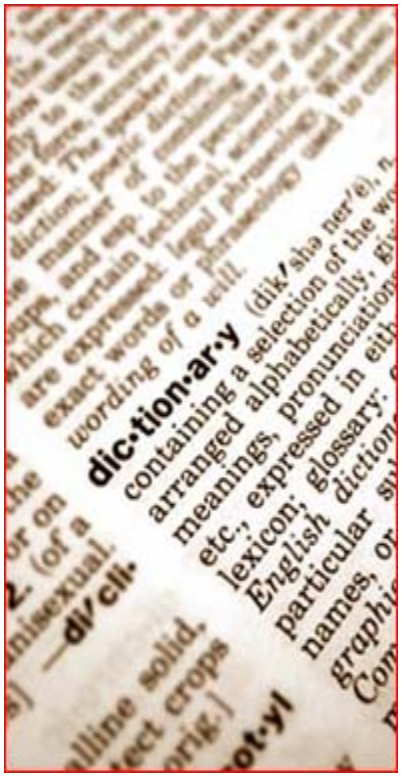
Licensed from CartoonStock.com

HA&W
HABIF, AROGETI & WYNNE, LLP
ertified Public Accountants and Business Advisors

Definitions:

R=Probability x Impact

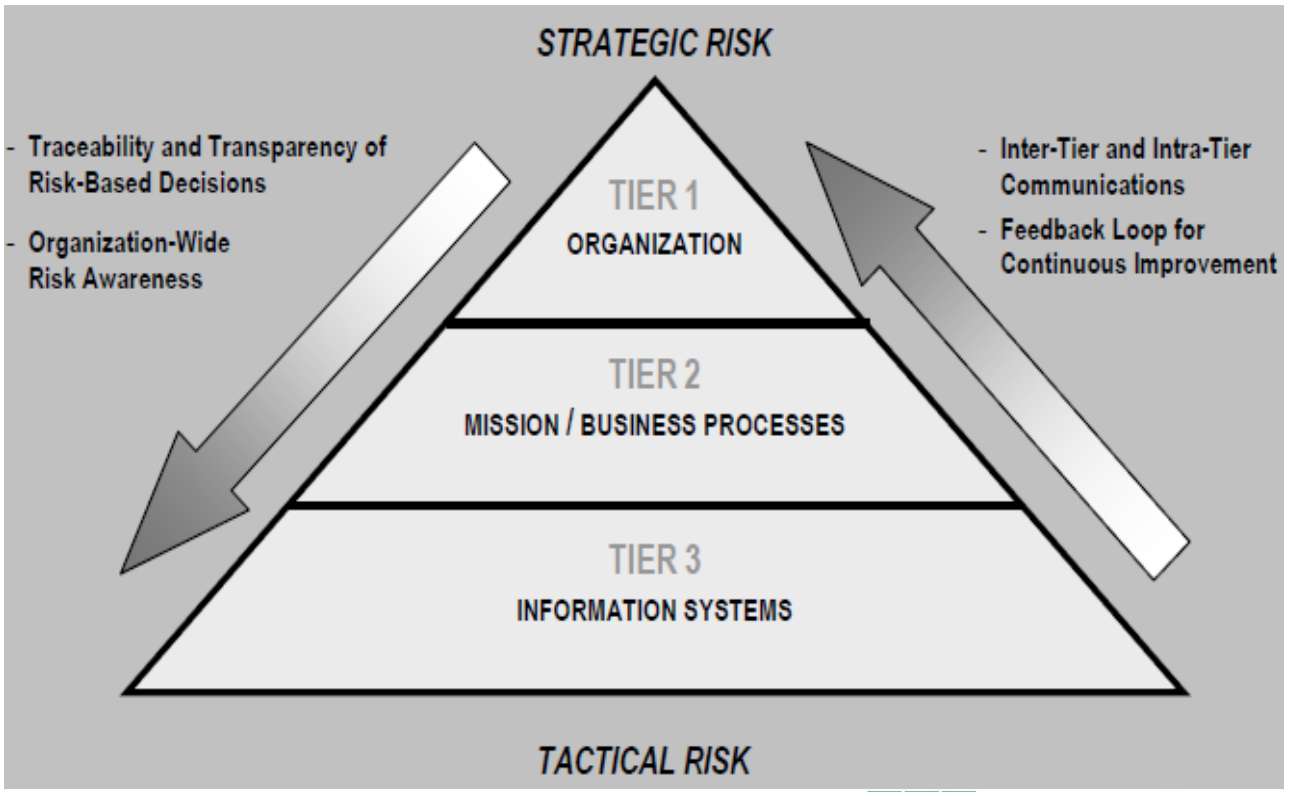
- **Risk**: Extent to which an entity is threatened by a potential event. (Note: Quantitative or Qualitative)
- **Risk Assessment**: Prioritization of risks based on probability and impact of an event.
- **Threat**: Circumstance with potential to adversely impact organizational operations, assets, individuals, and others.
- **Vulnerability**: Weakness in an information system, procedures, controls, or implementation.
- **Impact**: Magnitude of harm expected to result from the consequences of an event.
- **Probability**: Likelihood that a threat event will be initiated or will occur.
- **Predisposing conditions**: Condition which affects the probability that threat events, once initiated, result in adverse impacts.



http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk Management (RM) Hierarchy



Reference: NIST 800-30

http://www.linkedin.com/pub/scott-ritchie/2/308/260

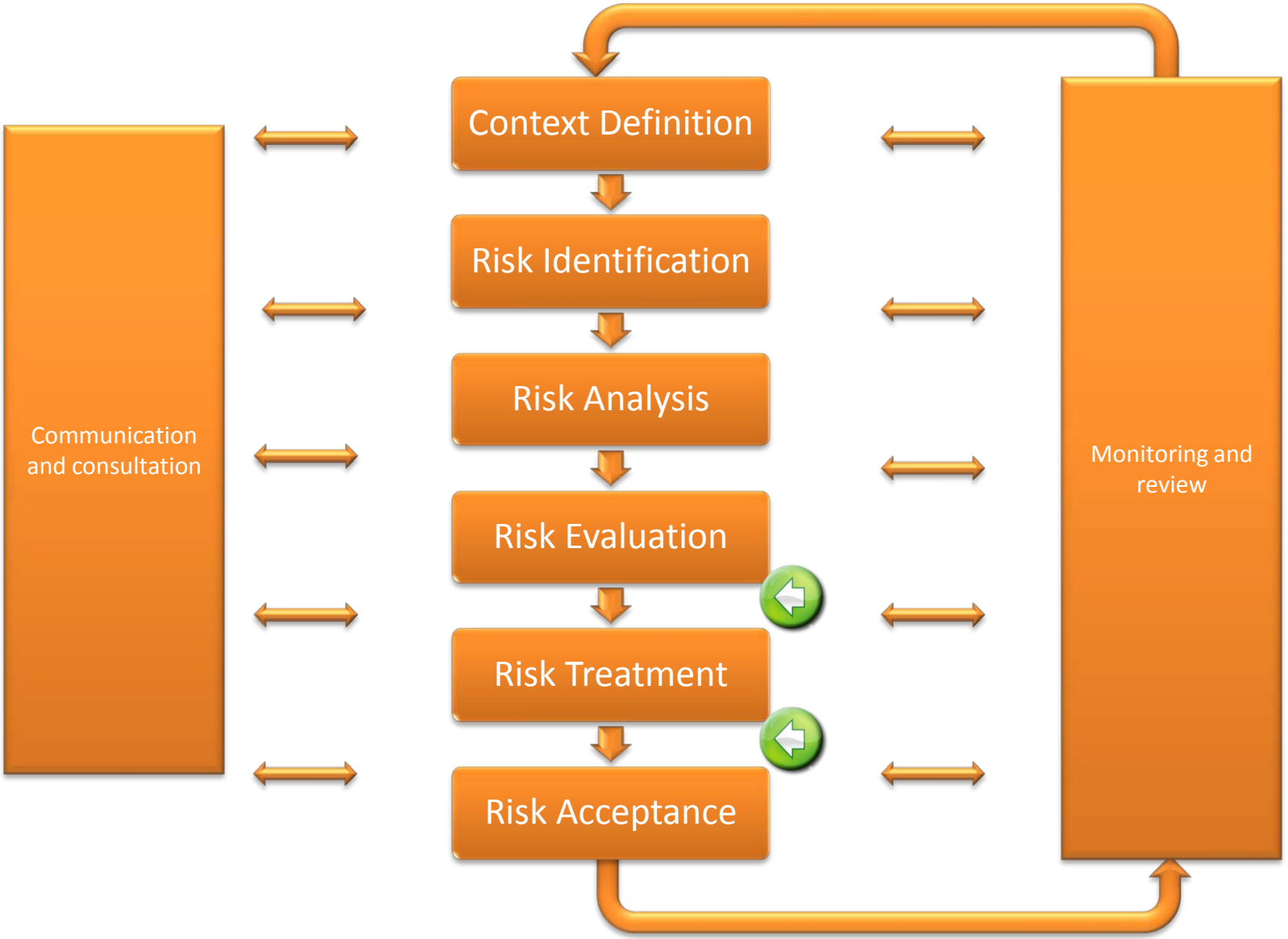
HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk Assessment Frameworks

OCTAVE	FAIR	NIST SP800-30	ISO 27005
1. Establish Risk Measurement Criteria 2. Develop an Information Asset Profile 3. Identify Information Asset Containers 4. Identify Areas of Concern 5. Identify Threat Scenarios 6. Identify Risks 7. Analyze Risks 8. Select Mitigation Approach	1. Identify scenario components • Identify asset at risk • Identify the threat community 2. Evaluate Loss Event Frequency • Calculate Threat Event Frequency (TEF) • Calculate Threat Capability (Tcap) • Estimate Control Strength (CS) • Derive Vulnerability (Vuln) • Derive Loss Event Frequency (LEF) 3. Evaluate Probable Loss Magnitude (PLM) • Estimate Worse Case Scenarios • Estimate Probable Lost Magnitude (PLM). 4. Derive and articulate Risk	1. System Characterization 2. Threat Identification 3. Vulnerability Identification 4. Control Analysis 5. Likelihood Determination 6. Impact Analysis 7. Risk Determination 8. Control Recommendations 9. Results documentation	1. Risk Identification • Identification of Assets • Identification of Threats • Identification of existing controls • Identification of vulnerabilities • Identification of Consequences 2. Risk Estimation • Assessment of consequences • Assessment of incident likelihood • Level of risk estimation 3. Risk Evaluation

http://www.linkedin.com/pub/scott-ritchie/2/308/260

ISO 27005: IT Risk Management



http://www.linkedin.com/pub/scott-ritchie/2/308/260

Understand the Organization

Management Commitment

Rationale for managing risk	Accountabilities for managing risk	Methods for resolving conflicting interests
Commit resources	Risk management performance metrics	Management Review
Response to an event or change in circumstances.	Risk Management Policy Communication	Democratization of Risk Management

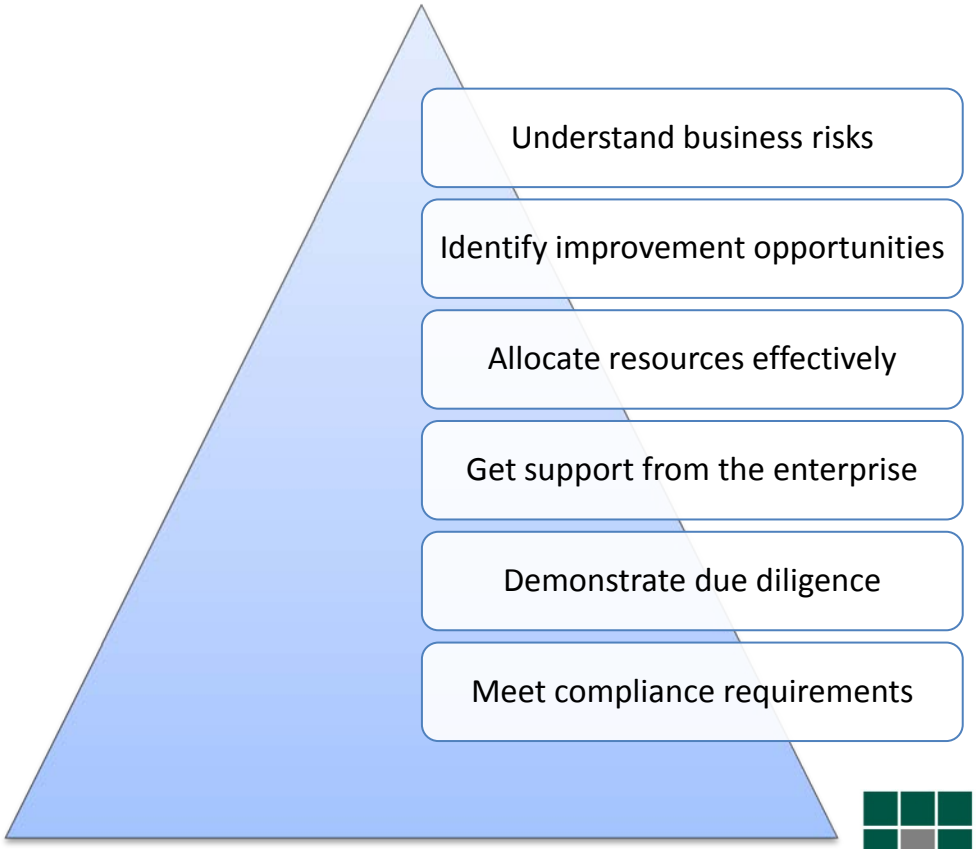
HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk Management Approach

Nature and types of causes and consequences	Likelihood and impact Criteria	How the level of risk is to be determined
Views of stakeholders	Risk Tolerance Level and Acceptance Criteria	Combinations of multiple risks

http://www.linkedin.com/pub/scott-ritchie/2/308/260

Objectives of Risk Assessment



http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Information Asset Inventory

- Anything of value that requires protection
  - People, Process, Technology
  - Information
  - Supporting Infrastructure
  - Business processes
- Data Sources:
  - Listings of Enterprise Applications
  - Listings of Databases
  - Software Inventory
  - Hardware Inventory
  - System Diagrams
  - Technical Design Documents

http://www.linkedin.com/pub/scott-ritchie/2/308/260

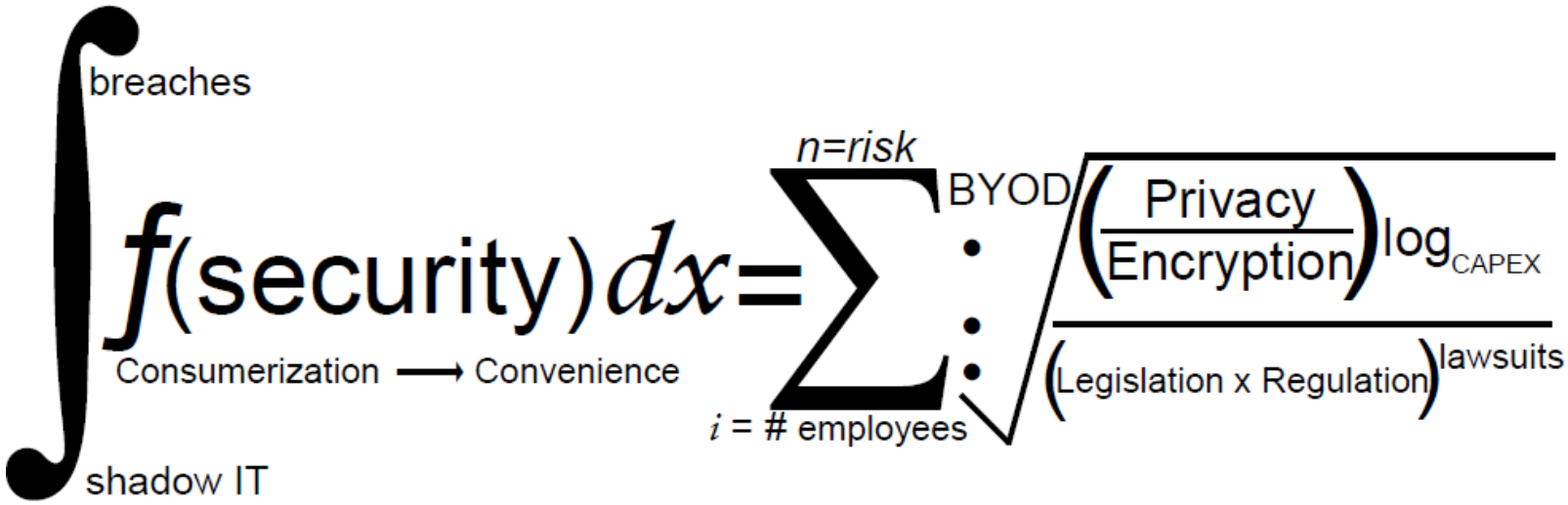
Example Asset Register

Asset Name/ Description	Asset Class.	DR Priority	Description	Exposure Level (H,M,L)
Personnel	High	1	Employees	M
Client PII	High	1	Personally Identifiable Information	L
Production Web server	Medium	1	Company primary web site (no sensitive data)	H

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Calculating Risk (perception)



Source: CSOOnline.com

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

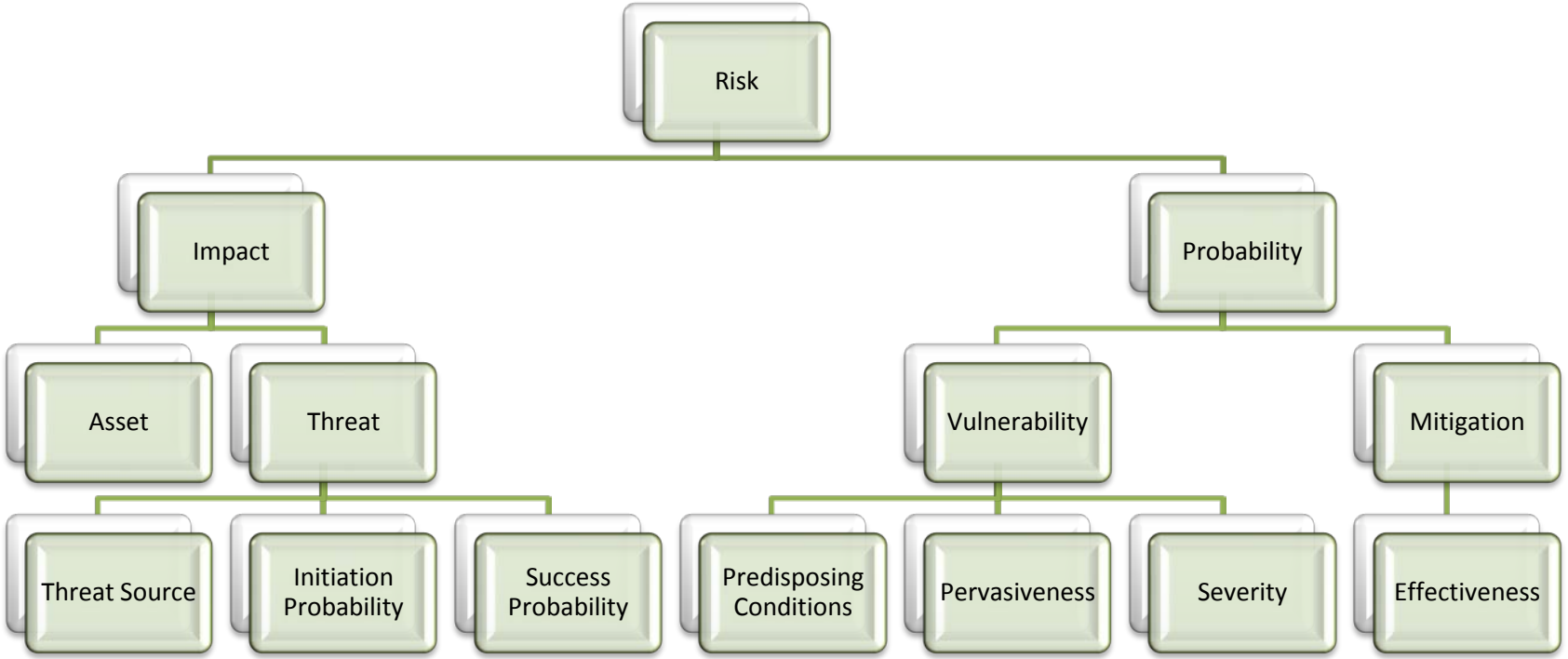
Calculating Risk

Risk = Impact X Probability

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Elements of Risk



http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk Identification

"Well he certainly does a very thorough risk analysis."

Licensed from CartoonStock.com

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk Identification Sources

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Assess Threats

- Deliberate Attacks
  - Intent
  - Capabilities
  - Operational constraints
  - Exploit characteristics
- Unintentional Exposures
  - Characteristics
  - Work Environment
  - Time constraints
- Natural
  - Fire
  - Water
  - Earth
  - Air

Likelihood Considerations

- Experience and statistics for threat likelihood
- Motivation and capabilities of the attacker
- Exposure to possible attackers
- Accident sources: geographical /weather
- Human errors and equipment malfunction
- Individual and aggregate vulnerabilities
- Effectiveness of existing controls

http://www.linkedin.com/pub/scott-ritchie/2/308/260

Vulnerabilities

- Organization
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

http://www.linkedin.com/pub/scott-ritchie/2/308/260

Impact criteria

- Asset classification
- Breaches of information security
- Impaired operations
- Loss of business and financial value
- Disruption of plans and deadlines
- Damage to reputation
- Breaches of requirements

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk evaluation criteria

- Strategic value of the assets
- Criticality of the assets
- Legal, contractual, and regulatory requirements
- Operational and business importance of confidentiality, integrity, and availability (CIA)
- Stakeholders expectations
- Damage to reputation

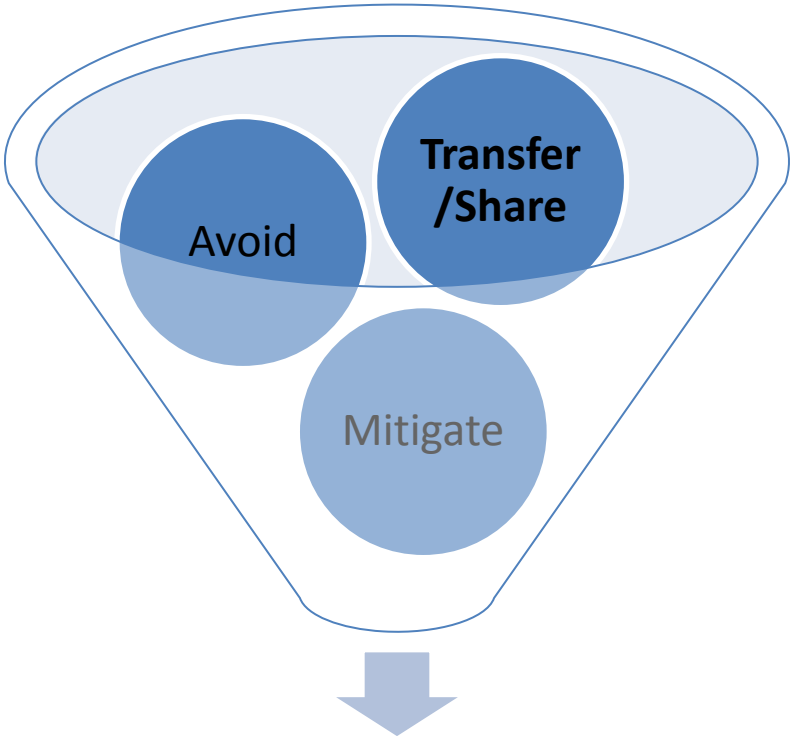
http://www.linkedin.com/pub/scott-ritchie/2/308/260

Example Risk Register

Threat	Predisposing Conditions	Vulnerable Entities	Confidentiality	Integrity (L,M,H)	Availability (L,M,H)	Overall Impact	Likelihood of Attack Initiation	Likelihood Success	Total Likelihood	Overall Risk Rating	Control Effective-ness
Lack of communication of Business and IT needs leads to unintended exposure of data.	Business objectives are not aligned with IT strategies.	Business Operations	H	H	H	H	H	H	H	H	M
Accidental or intentional duplication and retention of data leads to unnecessary exposure.	Sensitive documents are retained beyond useful life	All data sources.	H	M	M	H	H	H	H	H	L
Lost or stolen laptop leads to exposure of sensitive data.	No encryption on almost all laptops	All servers, network devices, and laptops.	H	L	H	H	H	H	H	H	M
Improper handling of data by employees, contractors, or vendors leads to exposure of sensitive data.	No formal privacy awareness, data handling, or information security training.	Employees, contractors, and vendors.	M	M	M	M	H	H	H	M	L

http://www.linkedin.com/pub/scott-ritchie/2/308/260

Risk Treatment



Accept

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Risk acceptance criteria

- Multiple thresholds and provisions for senior managers to accept risks
- Ratio of estimated benefit to the estimated risk
- Different acceptance criteria for different classes of risk
- May include requirements for future additional treatment

http://www.linkedin.com/pub/scott-ritchie/2/308/260

Report

- Executive Summary, Methodology, and Detailed Results
- Share results of assessment - present risk treatment plan
- Eliminates misunderstanding among decision makers and stakeholders
- Supports decision-making
- Improve awareness and provides new knowledge
- Co-ordinate with other parties and plan responses
- Give decision makers and stakeholders a sense of responsibility about risks

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Re-Assess Risks

- Assessments are an on-going exercise
- Track mitigation strategies
- Re-test control design/effectiveness
- Document test results, corrective actions, changes in business needs/requirements.

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Future

- Develop risk-aware mission and business processes
- Integrate into enterprise architecture development
- Acquire IT systems with high level of assurance
- Consider threats when deploying new technology
- Agile defense
- Implement robust continuous monitoring programs

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Questions

http://www.linkedin.com/pub/scott-ritchie/2/308/260

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

THANK YOU!

HA&W
HABIF, AROGETI & WYNNE, LLP
Certified Public Accountants and Business Advisors