A Taxonomy of Information Risk

William Saffady

www.saffady.com
wsaffady@saffady.com

Part 1–Risk terminology and concepts

- What is risk?
- Enterprise risk management
- Threat agents
- Vulnerabilities
- Risk response
- What is information risk?

What is Risk?

- Much discussed but no universally accepted definition
- ISO: “the effect of uncertainty on objectives” where uncertainty is a “deficiency of information” and the effect is a “deviation from the expected”
- Risk may have positive (speculative risk) or negative (pure risk) connotation
- Combination of threats, vulnerabilities, consequences
- Risk assessment
    - What can go wrong?
    - What can cause it to go wrong?
    - What will happen if it does go wrong?
- Possibilities range from high impact events with high probability of occurrence to low probability events with limited negative impact
- Reflecting uncertainty—most risks have variable rate of occurrence and variable impact

Enterprise Risk Management

- Coordinated program that treats risk management as part of organizational governance – aligned with strategic objectives
    - GRC alignment: Governance, Risk, Compliance
    - Supports governance's responsibility for prudent stewardship of assets
    - Addresses the principal-agent problem
    - Assign risk management authority—CRO or other: legal, compliance officer
- Incorporate risk awareness and management into all business activities and processes
- Anticipated benefits
    - Improved decision-making
    - Better oversight of risk-related behavior
    - Lower legal costs and fewer compliance violations

Threat Agents

- Have potential to harm an organizational asset
- Threat identification is a critical aspect of risk management
- May be internal or external, natural or human sources, malicious or accidental
- Variable likelihood of occurrence -- depends on motivation, capability, opportunity, uncontrollable factors
  - May be identifiable and predictable within limits
  - May arise from extremely unlikely events (“black swans”) or from unrecognized or underestimated risk sources
- Probability of occurrence must be balanced against consequences – business disruption, civil litigation, fines for regulatory non-compliance, loss of reputation, criminal prosecution

Vulnerabilities

- The probability that a threat exceeds the ability to resist it
- The basis for risk exposure – a threat poses no harm in absence of vulnerability
- Vulnerabilities must be identified and evaluated—a key aspect of risk assessment
    - Susceptibility (openness to attack by a threat agent)
    - Exposure (opportunity for attack by threat agent)
- May be based on natural events or caused by human action or inaction
    - Lack of required capabilities (unqualified staff)
    - Defects in business process (inadequate training or supervision)
    - Flawed system components (unreliable software or network security)
    - External factors (geographical location)

Risk Response

- Also termed “risk mitigation” or “risk treatment”
- Purpose: reduce exposure to negative consequences of a threat
- Inherent risk: level of risk before response; residual risk: level of risk after response
- Goal: to attain tolerable level of residual risk
- Response options
    - Risk acceptance – guided by organization’s risk appetite
    - Risk avoidance – an extreme form of risk aversion that seeks to eliminate threat, possibly by changing or discontinuing activities
    - Risk transfer – shifts risk to a third-party, usually insurance company, but also contractual provisions or warranties
    - Risk limitation – address specific vulnerabilities to minimize adverse consequences of a threat

What is Information Risk?

- Important topic at the nexus of risk management and information governance
- A specialized aspect of general business risk
- Identifies and assesses risks to an organization's information assets – an important category of organizational assets
- Strongly associated with information technology and cyber security but applies to information of all types in all formats
- Identifies and assesses threats, consequences, and vulnerabilities related to creation, collection, ownership, storage, retention, retrieval, and disclosure of information
- Information risk taxonomy—categorizes risks to facilitate identification and assessment

Part 2—Risk Taxonomy

- Creation and collection of information
- Loss of information
- Retention of information
- Retrieval and disclosure of information
- Ownership of information

Creation and Collection of Information

- Failure to collect information for submission to government agencies—exposes organization to fines or other penalties
- Unauthorized or excessive collection of personal information—non-compliance with data minimization requirements
- Illegal collection of non-public information – organization has trade secrets of others in its possession
- Creation or collection of information with objectionable content – exposes organization to workplace harassment as form of employment discrimination, tarnished reputation
- Creation or collection of information with defamatory or private content – litigation risk
- Creation or collection of poor-quality information—impact on decision-making, transaction processing, customer service, tarnished reputation

Loss of Information

- Vulnerability depends on two factors
    - Likelihood of occurrence, which varies with geography
    - Ability to recover lost information following disaster—backup copies are essential
  - Natural disaster: meteorological, geological, hydrological, climatological, extra-terrestrial– low likelihood but devasting consequences
  - Malicious human actions – software attacks, armed conflict, civil insurrections, vandalism, information theft
  - Accidents – may result from human error or technological malfunction
  - Fire: a threat in office buildings, record centers, data centers—may be accidental or intentional

Retention of Information

- Non-compliance with recordkeeping laws and regulations – exposure to fines, penalties, increased regulatory scrutiny
- Failure to preserve information that is relevant for litigation, government investigations, other legal proceedings
- Under-retention – Loss of useful information, negative impact on preservation of records of scholarly value
- Over-retention – increased recordkeeping costs, degrades performance of computer applications, increased effort to comply with discovery orders, violates laws and regulations that specify maximum retention periods
- Media instability and obsolescence

Retrieval and Disclosure of Information

- Failure to retrieve information needed for a given purpose—high likelihood
  - Poorly conceptualized or poorly articulated requirements
  - Faulty search strategy
  - Defective indexing
  - Errors in data
- Metadata mining – analysis of metadata to obtain additional information
  - Metadata embedded in documents
  - Includes additions, deletions, comments, names of authors or reviewers
  - Inadvertent disclosure can have harmful effects
  - A particular problem for legal discovery

Retrieval and Disclosure of Information

- Mandatory disclosure of information – exposes organization to regulatory compliance violations
  - Freedom of Information and Right to Know laws
  - Mandatory disclosure to government agencies
    - Anti-money laundering
    - Financial misconduct
    - Adverse drug events
    - Child abuse
  - Disclosure of PII to data subjects
- Prohibited disclosure of non-public information—PII, PHI, trade secrets, NDA restrictions, insider trading, professional-client privilege
- Prohibited cross-border transfer of information— personal data protection laws, blocking statutes
- Violation of data breach notification requirements

Ownership of Information

- Challenges to or infringement of intellectual property—copyrights, patents, industrial designs
- Work-for-hire doctrine—Who owns the information you create at work?
- Loss of trade secret status through disclosure—trade secrets vs. patent protection
- Data portability laws – allow data subject to take possession and ownership of personal information