Information Technology Risks in Today’s Environment

- Traci Mizoguchi
  Enterprise Risk Services Senior Manager,
  Deloitte & Touche LLP
Agenda

- Overview
- Top 10 Emerging IT Risks
- Summary
- Q&A
Overview

• Technology continues to increase in strategic importance and risk to organizations

• Rapid deployment of emerging technologies creates risk

• Regulatory requirements and scrutiny is ever increasing

• Deficiencies in IT controls can have a significant impact on the organization
Top 10 Emerging IT Risks

• By no means a comprehensive list

• Will vary by environment
  – May be greater/lesser risk depending on industry, technology, business processes, etc.

• This list is based on what we see in the marketplace

• Designed to get you thinking about your IT environments and risk assessment process

• List is in no particular order
1. Social Networking

**Issue**
Use of social media technologies is expanding into new areas. Examples include user communities, business collaboration, and commerce. Regulatory requirements are catching up (e.g. financial services organizations).

**Risk**
- Brand protection
- Unauthorized access to confidential data
- Regulatory or legal violations
- Current company policies may not readily apply

**Recommendation**
Historical audits are insufficient as risks are rapidly evolving. Need to complete an inventory of social media usage, and existing policies, procedures and controls. Draft and execute new audit plan based on emerging risks and current usage within the organization – may need to include the HR, IT, and Legal departments. Determine whether a training course should be delivered to employees.
2. Mobile Devices

Issue
Rapid expansion of number of devices, and functionality (e.g., 15+ million iPads in current circulation). mCommerce enabling technologies within companies introduces new risks as well.

Risk
• Loss / release of critical business data
• Security and identity management
• Application development challenges
• ERP integration issues

Recommendation
Historical audit procedures are insufficient. Need an inventory of all current allowable devices and corresponding policies & procedures. Evaluate effectiveness of “push” controls. Understand mCommerce activities and processes/technology. Ensure that controls are in place for lost devices.
3. Malware

Issue
Malware continues to increase in sophistication, and has more avenues for execution (e.g. mobile devices and traditional computing). Most PCs still provide local admin access. Work-at-home flexibility increases issues.

Risk
• Loss or theft of critical information
• Hardware impacts
• Cash impact
• Lost productivity

Recommendation
Understand organizational approach to malware identification, isolation, and remediation. Consider impacts beyond traditional spamware/firewalls (e.g., remote users, mobile devices). Consider update schedules and monitoring (beyond responsiveness to patch updates). Control contractor / consultant access to the corporate network.
4. End User Computing

Issue
End User Computing (EUC) applications continue to evolve given resource constraints of economic downturn. Increased scrutiny is being applied by auditors and regulators, particularly to financial models. False sense of security provided by current efforts.

Risk
• Misstated financial statements
• Unsupported decision making
• Regulatory concerns
• Loss or corruption of data

Recommendation
Understand current approach to managing and controlling EUCs. Policy-based approaches are typically insufficient. Evaluate use of technology and critical technical settings. Evaluate other program aspects including governance, security, management processes, and training/awareness.
5. Corporate Espionage

Issue
More specific targeted efforts (often for gain), assisted by increase in mobile computing technologies. Increased access to government defense toolkits. Specific verticals hardest hit – e.g. oil firms, gaming platform networks, defense contractors.

Risk
• Loss or release of corporate data
• Denial of service
• Intellectual Property loss

Recommendation
This should be a component of information security audits. SOX “monitoring controls” generally insufficient. Need to understand specific threats, user awareness, hardening of critical devices and access points (via firewalls and network traffic monitoring devices / software), vulnerability assessments, and detection/escalation procedures.
6. Project Backlog

**Issue**
Economic downturn caused decrease in IT investment and deferral of critical projects resulting in large project backlogs. Recent increase in resumption of large corporate IT projects, now being performed with reduced staff levels and/or weak project management oversight.

**Risk**
- Project delays or failure
- Completed projects shortchanging security and controls
- Failure to achieve business objectives
- Poor or inadequate vendor management

**Recommendation**
Current projects should be included in enterprise risk assessments and IT audit universe. Ensure that controls are built into projects; deferral until after project goes live creates substantial risk and remediation can be expensive.
7. IT Governance

Issue
Reduced enterprise IT support / budgets and increased ease of technology deployments has led to multiple “shadow IT” organizations within enterprises. Shadow groups tend to not follow established control procedures.

Risk
• Failure to comply with corporate IT policies and controls
• Operational impacts
• Information security risks
• Regulatory violations
• Duplication of efforts, increased costs and inefficiencies

Recommendation
Determine extent of shadow IT deployment. Identify applications and environments deployed outside of usual channels, and assess compliance with corporate policies. Evaluate and assess duplicative systems, licensing, and support issues.
8. Electronic Records Management (ERM)

**Issue**
Increased deployment of ERM solutions, with corresponding data conversions and process changes. Specific verticals more highly impacted (e.g., health care and financial services).

**Risk**
- Loss of data in conversion process
- Regulatory violations if inadequate controls exist
- Storage, retention, and forensic issues

**Recommendation**
Determine extent of ERM deployment. Identify impacted data and processes. Ensure data is mapped against existing data management strategies, policies and legal requirements. Evaluate storage controls and monitoring.
9. Data Management

Issue
Increased regulatory requirement for management and security of types of data. Lack of ability to identify types/location of enterprise data. Lack of robust data stratification schema to categorize sensitive data. Exacerbated by cloud deployments, shadow IT organizations, mobile computing, and electronic records management.

Risk
• Regulatory penalties
• Brand damage
• Increased cost of compliance

Recommendation
Evaluate current data management program. Assess level of adequacy to current business requirements and emerging regulations. Identify specific data management controls and perform focused audit procedures.
10. Cloud Computing

Issue
Proliferation of external cloud computing solutions, corporate- and user-based. Different deployments available; data, applications, services.

Risk
• Administrative access
• Data management – location/compliance/recovery/security
• Dependent upon availability of cloud provider and internet connection
• Investigative support
• Long-term viability

Recommendation
Identify cloud computing strategies deployed or planned. Determine applications and data impacted. Perform a risk assessment for the items impacted and determine the organization’s risk tolerance. Identify controls that mitigate risks identified above.
Summary

• Need to understand which items may be relevant in your business and technical environment

• Ensure that risk assessments (and internal audit’s universe) address relevant items

• Investigate / audit and prove that risks are adequately addressed to comply with regulatory requirements, company policies, and/or best practices
Contact

Traci Mizoguchi

trmizoguchi@deloitte.com

Office: (619) 237-6904

Cell: (617) 605-4752
Questions?