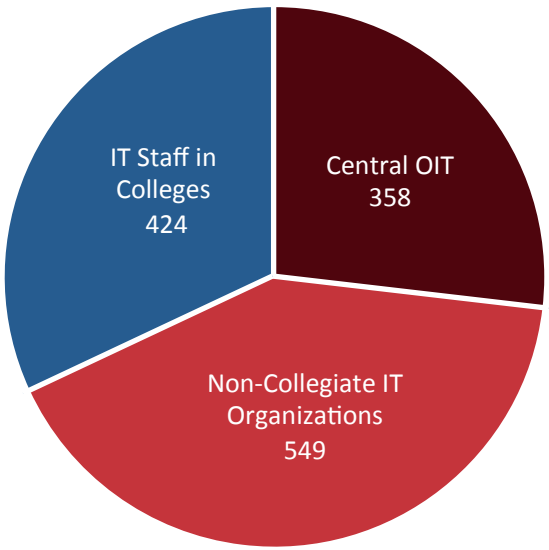
Information Technology Risk Profile

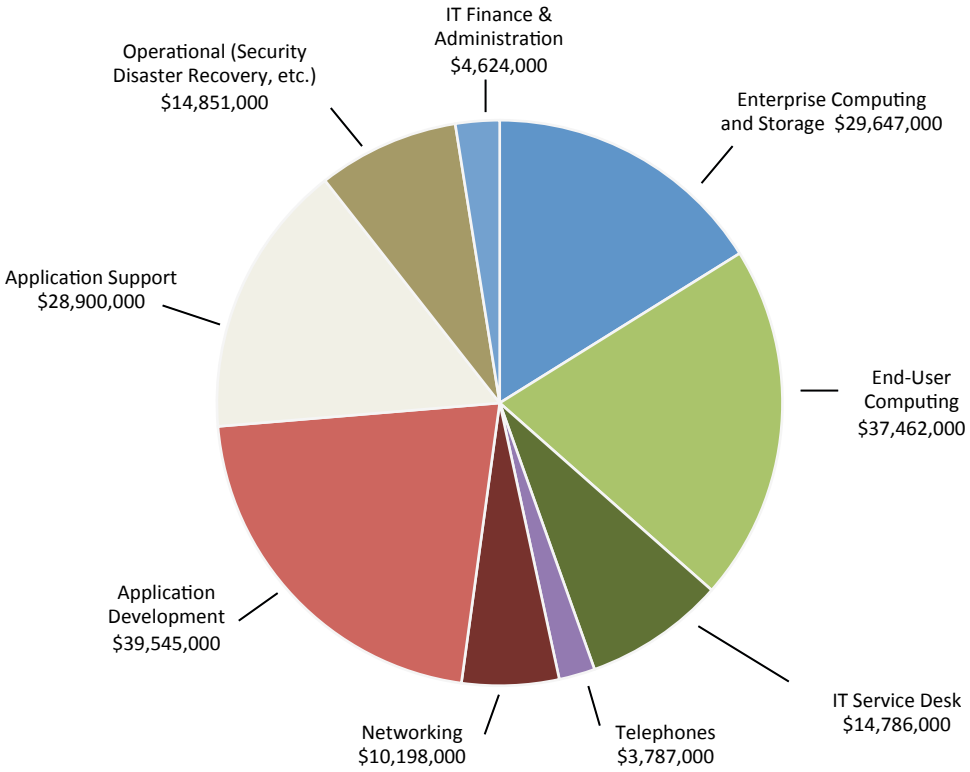
Presentation to the Audit Committee
May 9, 2013

UNIVERSITY OF MINNESOTA
Driven to Discover℠

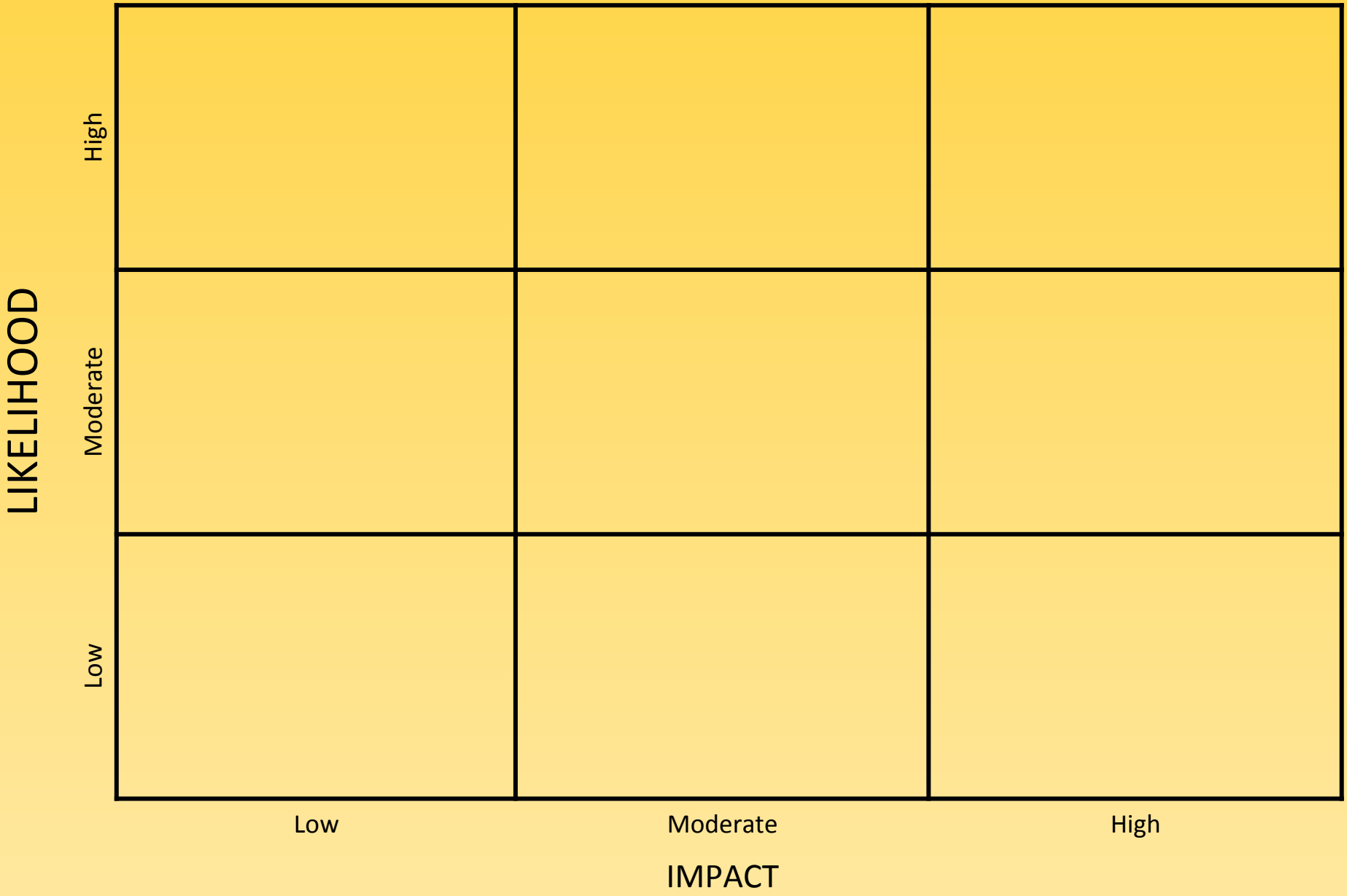
Overall Scope of IT at UMN

- 1,331 IT FTEs across the system
- Total IT expenditure $192,643,907





RISK PROFILE



RISK PROFILE

LIKELIHOOD

High

Moderate

Low

High

- Death or serious bodily injury due to University activity
- >$1,000,000 likely at issue
- Potential widespread and serious legal problem
- Requirement to report incident to an outside regulatory body with a reasonable likelihood of substantial financial or programmatic penalty
- Incidents highly likely to be accompanied by substantial negative publicity
- Circumstance is reasonably likely to result in a serious criminal charge against a University employee for University-related conduct

Moderate

- “Near miss” death or serious injury due to unsafe University activities
- Between $250,000 and $1,000,000 likely at issue
- University manager or supervisor credibly accused of misconduct
- Reasonable likelihood of a penalty from an outside body that is not substantial and is not anticipated to interfere with University programs in the judgment of the responsible reporting party and responsible vice president
- Potential for substantial negative publicity

Low **Moderate** **High**

IMPACT

RISK PROFILE

LIKELIHOOD

High

Moderate

Low

High

Probability of occurring multiple times a year

Moderate

Probability of occurring 1 time per 1 year

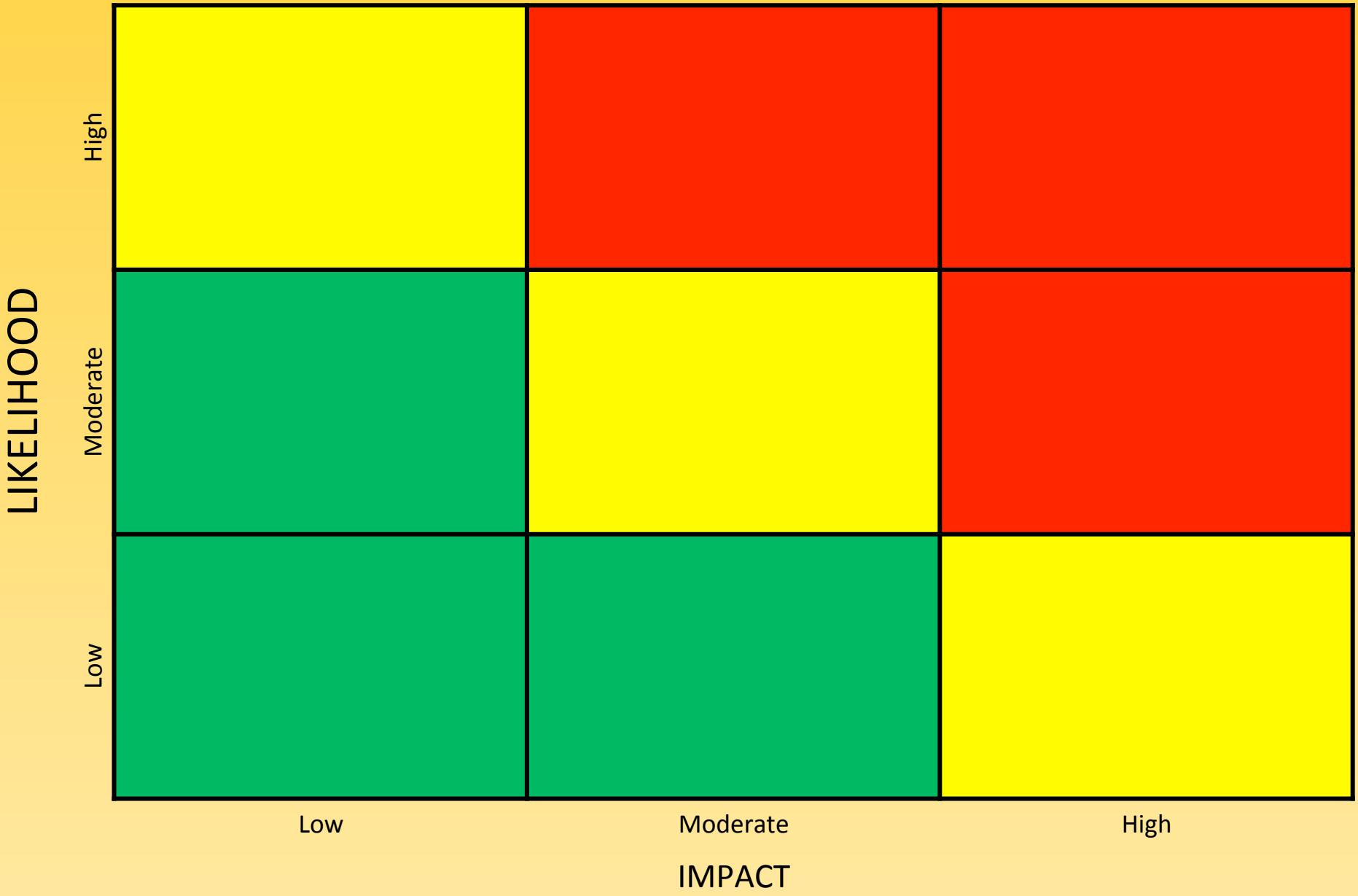
Low

Probability of occurring 1 time per 10 years

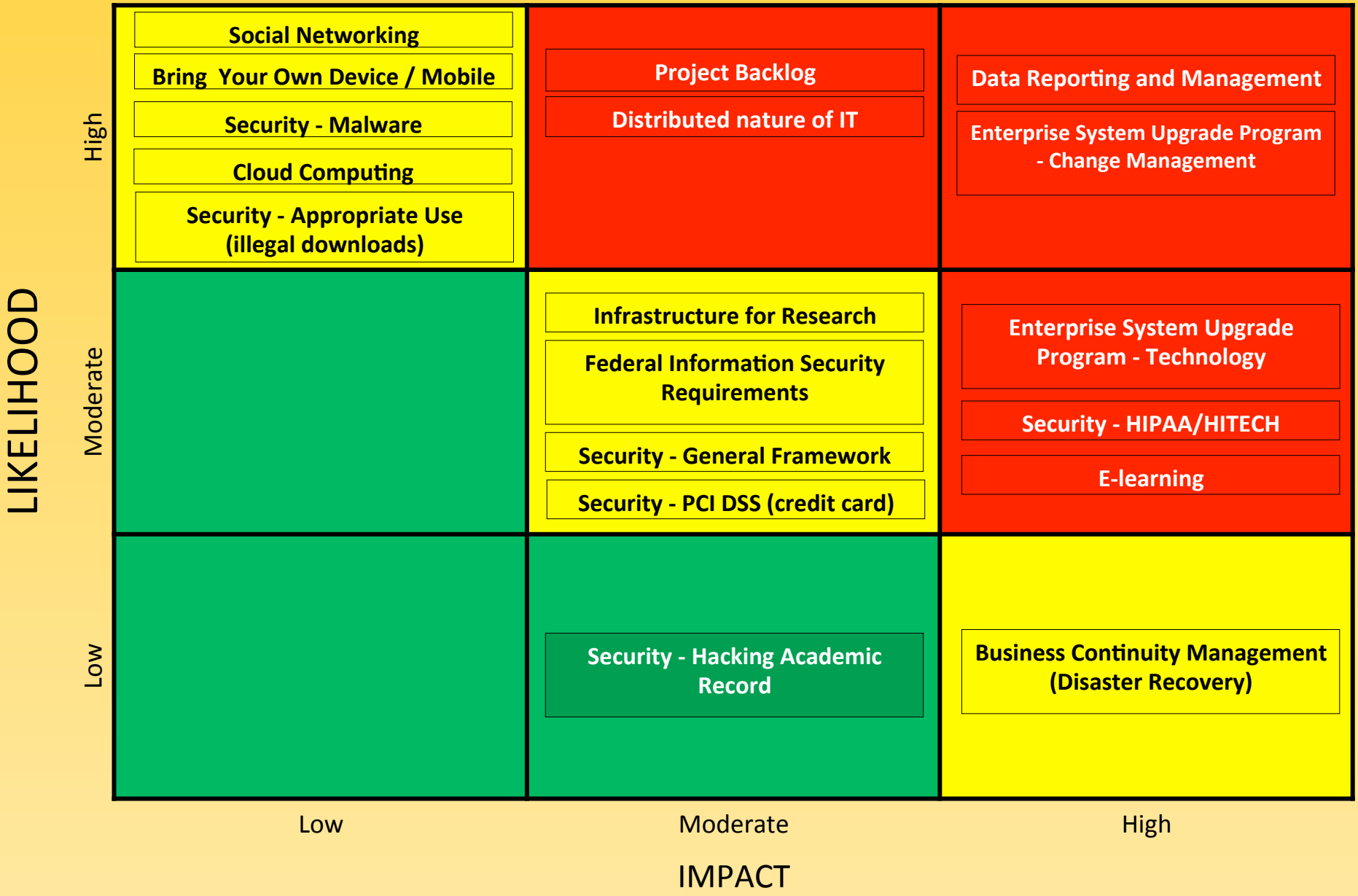
Low Moderate High

IMPACT

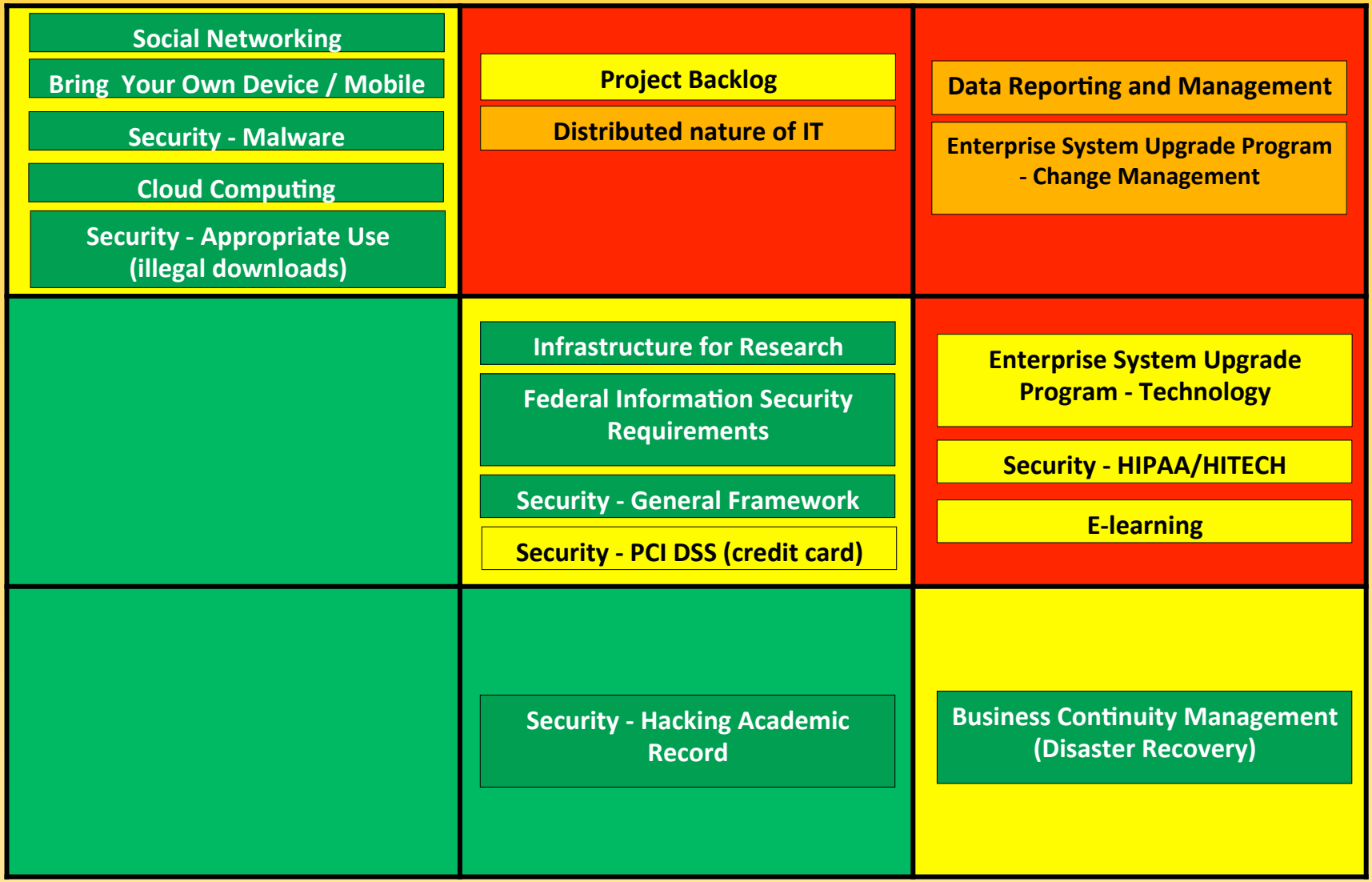
RISK PROFILE



INFORMATION TECHNOLOGY **INHERENT** RISK PROFILE



INFORMATION TECHNOLOGY **RESIDUAL** RISK PROFILE




Thank You

Data Reporting & Management

To enhance the University's ability to make real-time business decisions, the University is in the process of developing procedures for identifying required data and how it is acquired, validated, stored, protected, and processed. In addition, the University is ensuring the accessibility, reliability, and timeliness of its data.

RISKS

- Lack of single, accurate, and unified view of information
- Regulatory penalties
- Brand damage
- Increased cost of compliance
- Possible loss of institutional data

MITIGATION STRATEGIES

- Refocusing the Enterprise Data Management and Reporting (EDMR) team under the CFO to:
  - Evaluate the current data management program
  - Identify the need for enterprise reporting at the University and analytical reporting at the unit level
  - Identify strategy for delivering real-time data to end users
- As part of the Enterprise System Upgrade Program (ESUP), enhanced reporting functionality is expected in 2015/2016

Enterprise System Upgrade Program: Technology

The University of Minnesota is collaborating with an implementation partner to implement several changes to our Finance, Student, and HR systems. In addition, we are deploying a new self-service portal and enhanced reporting.

RISKS

- Significant schedule delays cause inability to update PeopleSoft system, impacting the University's ability to process student loans and payroll.
- Unclear scope leads to cost overruns or schedule delays
- Significant schedule delays cause continued dual development in old and new technologies, and additional ERP vendor support costs.

MITIGATION STRATEGIES

- Integrated project team chaired by college Dean and the Vice Presidents of Human Resources, Finance, and Information Technology and Vice Provost Undergraduate Education
- Utilize an implementation partner for technical skills

Enterprise System Upgrade Program: Change Management (Culture)

The Enterprise System Upgrade Program will impose significant changes to how end users interact with the ERP systems that support the University. Early engagement is critical to meeting user satisfaction. These changes will be substantial and may stress the institution.

RISKS

- Significant institutional stress resulting in media stories
- Lack of user understanding resulting in loss of productivity
- Unrealized / Unrealistic expectations for improved data reporting
- Unmanaged timeframe expectations

MITIGATION STRATEGIES

- Proactively implement an organizational change management program to help the institution through this difficult transition
- Clearly communicate project timeline (go live in late 2014 and early 2015 with one to two years of optimization)

Distributed Nature of IT

Historic issues from central IT services and increased ease of technology deployments has led to multiple “shadow IT” systems within the institution. Distributed groups tend to develop independent, redundant systems.

RISKS

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

MITIGATION STRATEGIES

- Creating a community of “we” across all of IT
- Dotted-line, clearer governance process
- Huron Consulting is benchmarking UMN IT investment relative to our peers and making recommendations
- Consolidate commodity functions (Network, Helpdesk, etc.)
- Establish an enterprise architecture and institutional technology standards

Project Backlog

Seeing a decrease in IT investment and deferral of critical projects, resulting in large project backlogs. Recent increase in resumption of large IT projects, now being performed with reduced staff levels and/or weak project management oversight.

RISKS

- Project delays or failure
- Completed projects shortchanging security and controls
- Failure to achieve business objectives
- Poor or inadequate vendor management
- Poor or inadequate end-user testing and/or change management

MITIGATION STRATEGIES

- IT governance process should set priorities
- Ensure that controls are built into projects to ensure proper executive support and agreement on cost/scope/schedule
- Current large projects should be included in enterprise risk assessments and IT audit

HIPAA / HITECH

The use of health information for administrative, research, gifting and other Institutional related purposes is increasing rapidly. This increased usage increases the risks for controlling and securing health information.

RISKS

- Regulatory penalties
- Brand damage
- Reduced research funding from NIH and others
- Research collaborations
- Negative impact to gifting

MITIGATION STRATEGIES

- Evaluate current state of health information usage and controls
- Assess level of adequacy to current business requirements and emerging regulations
- Identify specific controls and perform focused risk assessments
- Establish enterprise architecture and technology standards

Security: PCI DSS (Credit Card)

Security for credit cards and compliance with the Payment Card Industry Data Security Standard (PCI DSS) presents challenges. Additionally, the quantity of merchants and their unique business needs increase the complexity in meeting the standards University-wide.

RISKS

- Penalties due breach of confidential information or lack of compliance
- Negative publicity of a significant breach
- University merchants awareness of existing security practices

MITIGATION STRATEGIES

- University merchants, Information Technology and the Controller's office work closely together to address PCI DSS compliance requirements and implement systems that address security and compliance gaps
- Based on annual transaction volume, the University is in the process of moving from a Level 4 to a Level 2, which will require increased external oversight

Infrastructure for Research

Emerging fields in research are dependent on technology infrastructure.

RISKS

- Inability to compete for research grants because of lacking research cyberinfrastructure
- Inability to maintain integrity and availability of key research information

CONTINUE LEADERSHIP:

- UMN is one of the first Universities in the world to go to a 100Gbps Wide Area Network
- UMN is considered a high performance network leader, providing network services to the State of Minnesota (including K-12, MnSCU through the Minnesota Learning Network) and to the five-state region
- UMN is a charter member of Internet2 , and through the establishment of the University-conceived Northern Lights GigaPoP, high-profile state partners such as the Mayo Clinic, the Hormel Institute, and others now have access to local, national, and international high performance research networking capacity
- UMN led the creation of the BOREAS network and currently provides network engineering expertise and fiscal agent responsibility for this regions optical network (U-Wisconsin, UChicago, Iowa St, etc.)
- UMN offers all faculty and staff “reasonable” data storage without quota

Federal Information Security Requirements

Faculty are signing contracts outside of Sponsored Projects Administration (SPA) that commit to FISMA. It is not possible for non-feds to accredit FISMA compliant systems. The key issue is in the program offices in the granting agencies.

RISKS

- Brand damage
- Regulatory penalties
- Research collaborations
- Constrained research funding

MITIGATION STRATEGIES

- Identify contracts with FISMA regulatory compliance requirements
- Perform risk assessments on identified FISMA grants
- Assess appropriate controls
- Collaboration between SPA, Export Controls Officer, and IT

Security: General Framework

As information technology advances rapidly, the University's security framework can work to increase the flexibility of our security controls in order to adapt to the business and security needs of the environment.

RISKS

- Insufficient security controls for high risk data and systems
- Ineffective controls for lower risk data and systems
- Frustrated users and system administrators

MITIGATION STRATEGIES

Implement our security framework to be based on the International Security Standard ISO 27001/27002. These efforts will work to increase our flexibility and improve our security posture by advancing our security risk management, exception management, data classification, and technical security standards

Social Networking

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

RISKS

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

MITIGATION STRATEGIES

- 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 the Office of the General Counsel (OGC)
- Determine whether a training course should be delivered to employees

Bring Your Own Device / Mobile

Rapid expansion of number of devices and functionality (e.g., 15+ million iPads in current circulation). Student, faculty, and staff expect to use consumer devices for any desired activities (including instructional purposes).

RISKS

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

MITIGATION STRATEGIES

- Historical audit and security procedures are insufficient. We must move from “controlled technology” to “educated user”
- Diversity of devices as a security strategy (no homogeneous attack vector)
- Evaluate effectiveness of “push” controls
- Ensure that controls are in place for lost devices

Security: Malware

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.

RISKS

- Loss or theft of critical information
- Hardware impacts
- Financial impact
- Lost productivity

MITIGATION STRATEGIES

- Increase training to end users around phishing and safe practices of online computing
- Understand organizational approach to malware identification, isolation, and remediation
- Consider impacts beyond traditional spamware/firewalls (e.g., remote users, mobile devices)

Cloud Computing

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

RISKS

- Poor quality or unrealized cost savings from cloud initiatives
- Data management – location/ compliance/recovery /security
- Dependent upon availability of internet connection
- Investigative support
- Long-term viability

MITIGATION STRATEGIES

- Partner with peer institutions on cloud strategies that work well with higher education
- Work with central purchasing to ensure distributed IT units understand integration costs between cloud services and UMN systems
- Establish enterprise architecture and technology standards

Security: Appropriate Use (Illegal Downloads, etc.)

University community members may inadvertently or intentionally misuse University data or systems in a way that violates our appropriate use policy and laws that prohibit theft, copyright infringement, or data privacy.

RISKS

- Penalties for violation of Digital Millennium Copyright Act (DMCA)
- Regulatory or legal violations
- Loss / release of confidential data

MITIGATION STRATEGIES

- Continue to provide security awareness and education on our policies and processes and the regulations that govern the use of data and systems
- Continue to track and monitor security incidents. Also provide response and notification where appropriate
- Rely on a mature DMCA notification process to meet our legal obligations

Business Continuity Management (Disaster Recovery)

The University must plan for disaster scenarios including being able to restore services in a reasonable timeframe from probable natural catastrophes or technology failures.

RISKS

- Revenue loss
- Brand damage
- Potential loss of mission-critical data
- Regulatory penalties

MITIGATION STRATEGIES

- Two geographically separate data centers for primary and recovery services for the business critical systems.
- Disaster recovery group is updating the recovery plans as part of the emerging information security framework.
- Implementing a tiered approach for which services must be restored in what timeframe.

Security: Hacking Academic Records

More specific targeted efforts (often for personal gain), assisted by downloadable hacking technologies that require little to no hacking abilities. Students will attempt to gain access to Moodle or PeopleSoft to modify their academic record.

RISKS

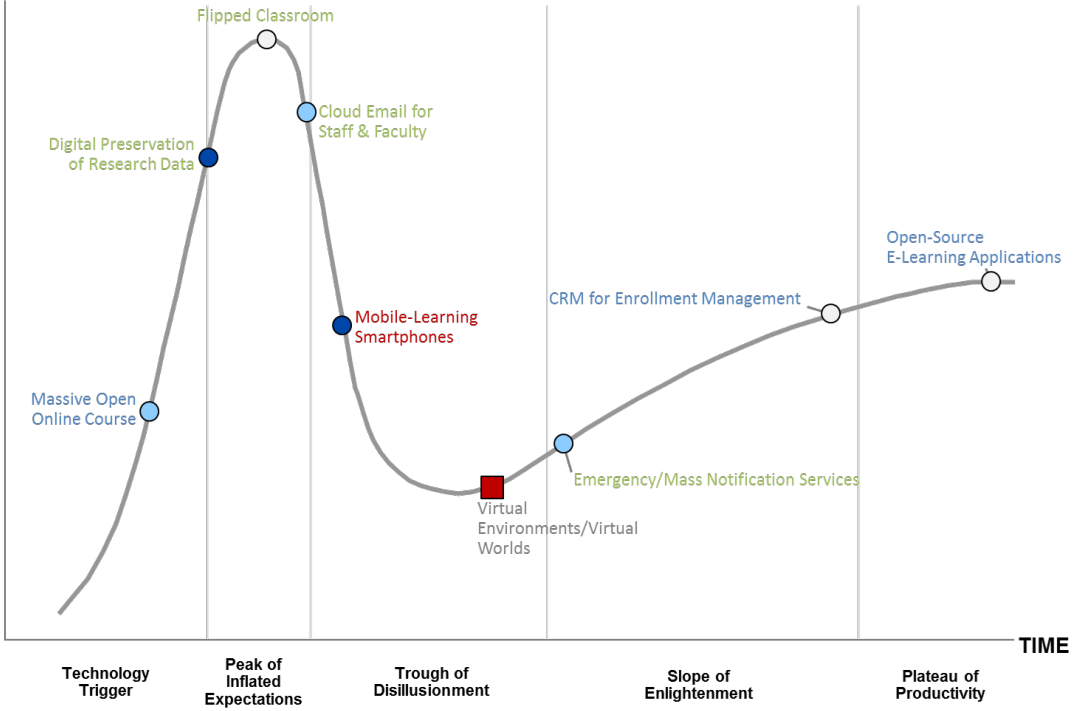
- Loss of integrity of institutional academic credibility
- Loss or release of institutional data
- Denial of service

MITIGATION STRATEGIES

- This should be a component of information security audits. Specifically the ISO “monitoring controls” around critical systems
- 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
- Log collection, log management, and auditing of logs to identify tampering

Technology Implications of E-Learning Trend

The pace and scope of disruptions in e-learning are increasing. Entrenched teaching practices and priorities limit faculty exploration and institutional success factors.



RISKS

- Misaligned academic technology investments
- Ineffective use of technology to enhance learning, retention, and enrollment growth
- Brand damage

MITIGATION STRATEGIES

- Use hype cycle and pilot projects to drive discovery and investment
- Expand academic technology support services to partner with faculty
- Commit technologists to support change management strategies from the Provost's Office