Risk Management

Who I Am

- B.S. Business Administration
  - MIS
- Master of Business Administration (MBA)
  - Information Assurance
  - Consulting
  - SFS Scholar
  - School of Nursing Graduate Assistant
  - Security Development Track
- Department of Homeland Security
  - NPPD, CS&C, +2-3 more

I am not representing the United States Government.
United States Government does not necessarily endorse, support, sanction, encourage, verify or agree with the comments, opinions, or statements of the following presentation.

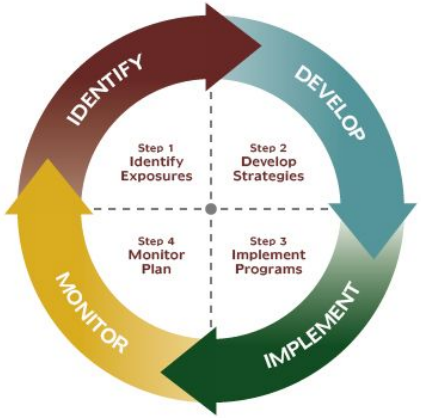
What is Risk?

Risk & Agenda

- is the potential of losing something of value
- Risk Process or Risk Management Life Cycle
- Risk = Likelihood X Impact
  - Likelihood - chance of a risk event occurring
  - Impact - Financial impact of the risk event
- Risk Appetite & Tolerance
- Risk Register
- Security Frameworks
- Compliance


Identify & Analyze Exposures
Examine Risk Management Techniques
Select Risk Management Technique
Implement Techniques
Monitor Results
Risk Management

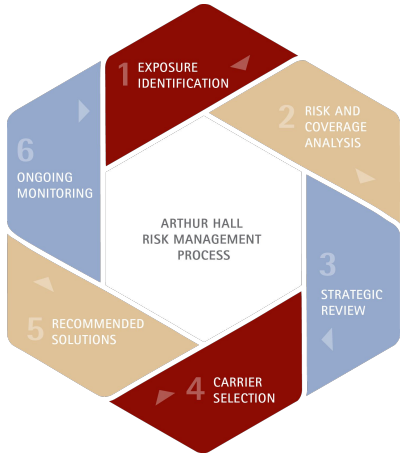

ASSESS RISK
IDENTIFY RISK
RISK MANAGEMENT PROCESS
CONTROL RISK
REVIEW CONTROLS


IDENTIFY
DEVELOP
IMPLEMENT
MONITOR
Step 1 Identify Exposures
Step 2 Develop Strategies
Step 3 Implement Programs
Step 4 Monitor Plan

WARNING!


Risks Identified
•Scope defined
•SWOT
•Checklists/tools
•Experience
•Interviews
Risks Prioritized
•Impact
•Probability
Risks Grouped By Categories
•Financial
•Schedule
•Quality
•Scope
Risk Analysis & Response
•Qualitative
•Quantitative
•Decision Trees
•Contingency Time and Costs
Risks Response
•Mitigate: Enhance Opportunities and Decrease Threats
•Log/Plan actions & alternatives
Risk Monitoring
•Know risk triggers
•Determine if assumptions are still valid
•Corrective actions
RISK MANAGEMENT CYCLE


Identifiy risks
Risk assess & analyze
Plan action
Implement
Measure, conrol and monitor
Risk management


1 EXPOSURE IDENTIFICATION
2 RISK AND COVERAGE ANALYSIS
3 STRATEGIC REVIEW
4 CARRIER SELECTION
5 RECOMMENDED SOLUTIONS
6 ONGOING MONITORING
ARTHUR HALL RISK MANAGEMENT PROCESS

Mini Case-Study

Your team (4 people) have been hired by SUNY UB to implement a security framework for various compliance.

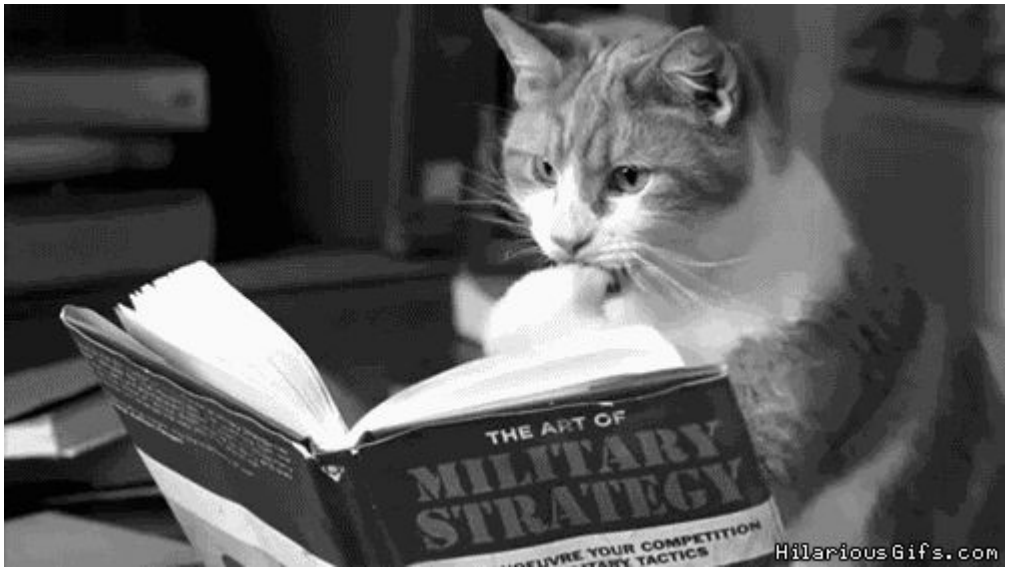
First things first, you will need to setup a risk management plan.

SUNY UB is a large organization, one of the largest university of the SUNY system. ~30,000 Students; ~6,000 Employees, ~2,500 Faculty, ~$716M Budget, ~12 Schools, ~40 Departments.

Let’s discuss

Planning

- Scope & boundary
- Resources
- Criteria
- Policy
- Enforcement
- Information Classification and Handling



Risk Management

Information Security Policies

Organization of Information Security

Human Resources Security

Asset Management

Access Control

Encryption

Physical and Environmental Security

Operations Security

Communications Security

System Acquisition, Development, and Maintenance

Supplier Relationships

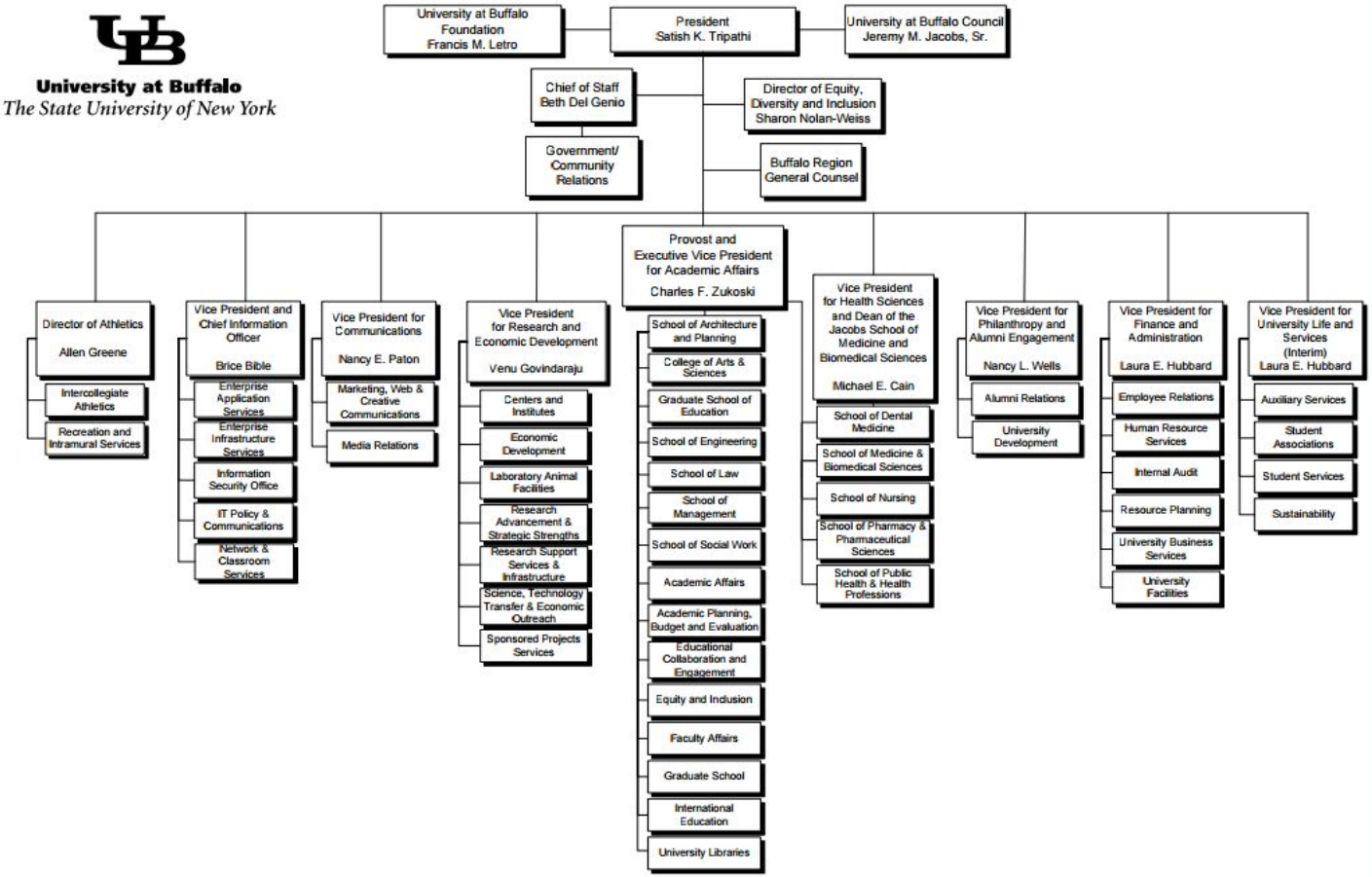
Information Security Incident Management

Information Security Aspects of Business Continuity Management

Compliance

Career and Workforce Development

University at Buffalo
The State University of New York



Last Updated: July 2016

Mini Case-Study

Active Directory (User Management)	Students’ Computers
Exchange (Email)	Wifi
File Servers	UBLearns
Print Servers	
VoIP System	
Network (Switches & Routers)	
Workstations	
Server Rooms	
Offices	

Assets

Inventory

Ownership

Acceptable Use

Impact to the business

Physical Access

Network

User

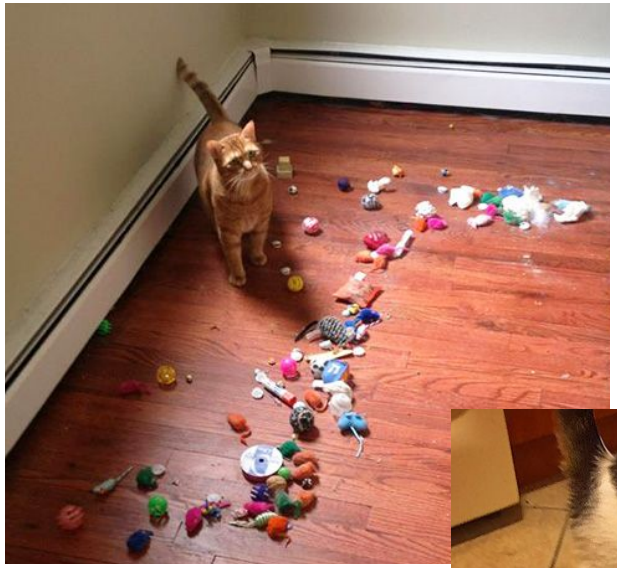
Software

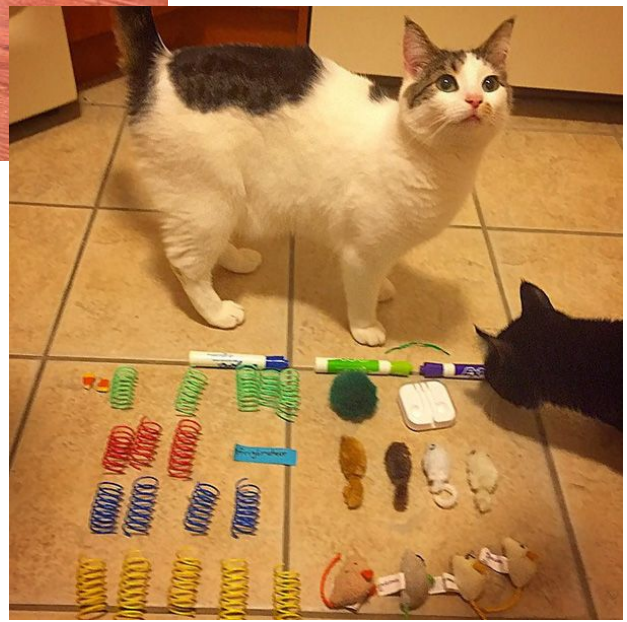
Hardware

Operational

Procedural and Policy

Information and Data





Mini Case-Study

Active Directory (User Management)	Students’ Computers
Exchange (Email)	Wifi
File Servers	UBLearns
Print Servers	Research Assets
VoIP System	Hypervisor (Virtualization)
Network (Switches & Routers)	Classrooms
Workstations	Software
Server Rooms	Sensitive Data/Information
Offices	UBHub

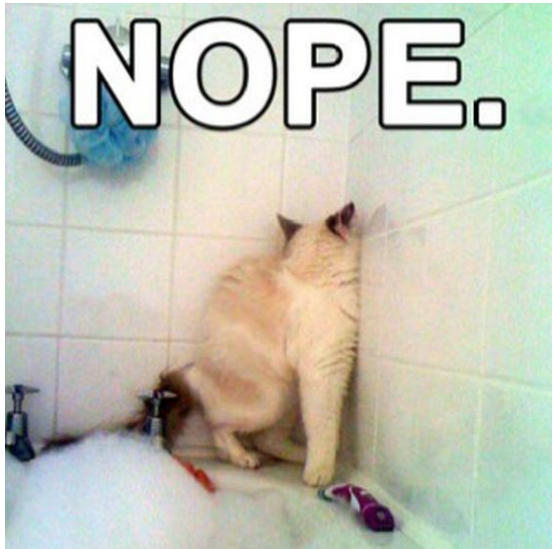
Mini Case-Study

Asset	Asset Inventory & Use
UBHub	- Students' PII, Grades, Schedule - Employee Info - Databases & ODBC - Multiple Privilege & Regular Users
Exchange (Email)	- PII?, Privacy, Grades? - Conversations - Personal & Business - Research - Multiple Privilege & Regular Users
Server Rooms	- Hypervisor (Virtual Machines) - Network Equipment - Users with Physical Access - Data & Info

Threats

Internal to our organization

o Budget loss for needed projects
o Systems growing overly complex
o System failures
o Staff turnover
o Insider threats
o Politics/Agendas



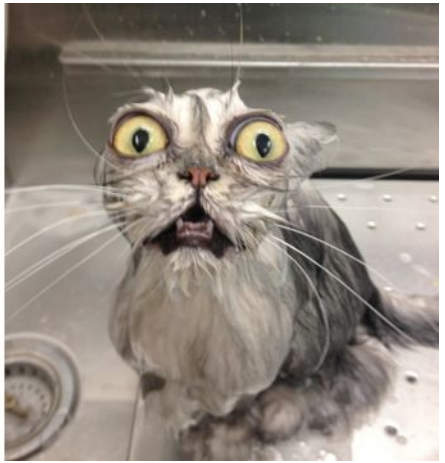
External to our organization

o Regulatory
o Legal
o Environmental / Weather related
o Utility related
o Natural disasters
o Economic
o Geo-political
o Civil unrest
o Cybersecurity events

Vulnerabilities

- Similar to Threats
- Weaknesses or gap
- Not just technical controls
- Usually specific

- **What is the Likelihood of exploitation?**
- **How can it be exploited?**

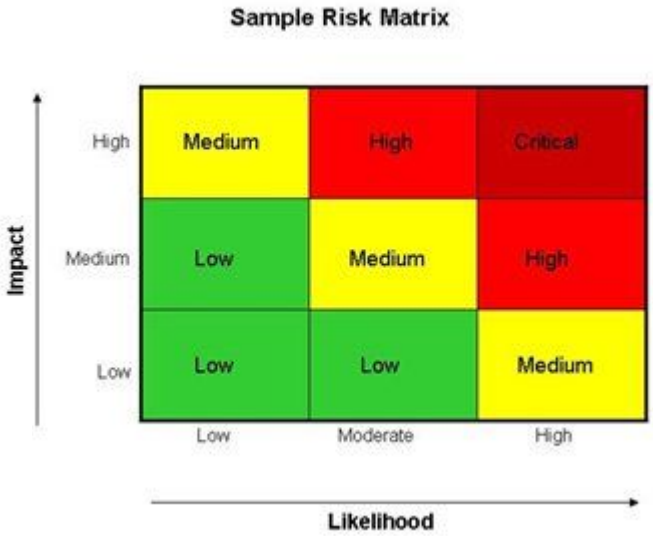


Mini Case-Study

Asset	Asset Inventory & Use	Threats	Vulnerabilities
UBHub	- Students' PII, Grades, Schedule - Employee Info - Databases & ODBC - Multiple Privilege & Regular Users	- Failure - Insider Threats - Overly Complex - Regulations and Legal	
Exchange (Email)	- PII, Privacy, Grades - Conversations - Personal & Business - Research - Multiple Privilege & Regular Users	- Regulations and Legal - System Failure - Complexity - Staff Turnover - Insider Threats	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII
Server Rooms	- Hypervisor (Virtual Machines) - Network Equipment - Physical Access Needed - Data & Info	- Natural Disasters - Utilities - Civil Unrest - Staff Turnover - Budgets, $$$$	- Physical Access - Location - Older HVAC - Older equipment - No Documentation

Risk Identification & Risk Analysis

- Follow consistent criteria and measurements
- Prioritize and plan (risk treatment)
- Risk Register & Matrix
- Impact
- Likelihood
- Security Frameworks



Mini Case-Study

Asset	Threats	Vulnerabilities	Impact	Likelihood	Risk
UBHub	- Failure - Insider Threats - Overly Complex - Regulations and Legal	- Too much access - No Documentation - Misconfigured - Lack of Knowledge	Medium	Low	Medium
Exchange (Email)	- Regulations and Legal - System Failure - Complexity - Staff Turnover - Insider Threats	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII	Medium	Low	Medium
Server Rooms	- Natural Disasters - Utilities - Civil Unrest - Staff Turnover - Budgets, $$$$	- Physical Access - Location - Older HVAC - Older equipment - No Documentation	High	Medium	High

Mini Case-Study

Asset	Threats	Vulnerabilities	Impact	Likelihood	Risk
UBHub	- Failure - Insider Threats - Overly Complex - Regulations and Legal	- Too much access - No Documentation - Misconfigured - Lack of Knowledge	$1.5M	3	$4.5M
Exchange (Email)	- Regulations and Legal - System Failure - Complexity - Staff Turnover - Insider Threats	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII	$1M	2	$2M
Server Rooms	- Natural Disasters - Utilities - Civil Unrest - Staff Turnover - Budgets, $$$$	- Physical Access - Location - Older HVAC - Older equipment - No Documentation	$3M	6	$18M

Risk Response

Avoid

Transfer/Share

Mitigate

Accept

Mini Case-Study

Asset	Vulnerabilities	Risk	POA&M or Risk Treatment
UBHub	- Too much access - No Documentation - Misconfigured - Lack of Knowledge	Medium	- Restriction of Users (Least Privilege Principle) - Documentation - Within a year
Exchange (Email)	- Misconfigured, Patching behind - Too much access - Lack of knowledge - Stored PII	Medium	- Restriction of Users (Least Privilege Principle) - Documentation - Encryption - With two years
Server Rooms	- Physical Access - Location - Older HVAC - Older equipment - No Documentation	High	- Replacement of HVAC and equipment - Documentation - Access Control - Card System - With 6 months

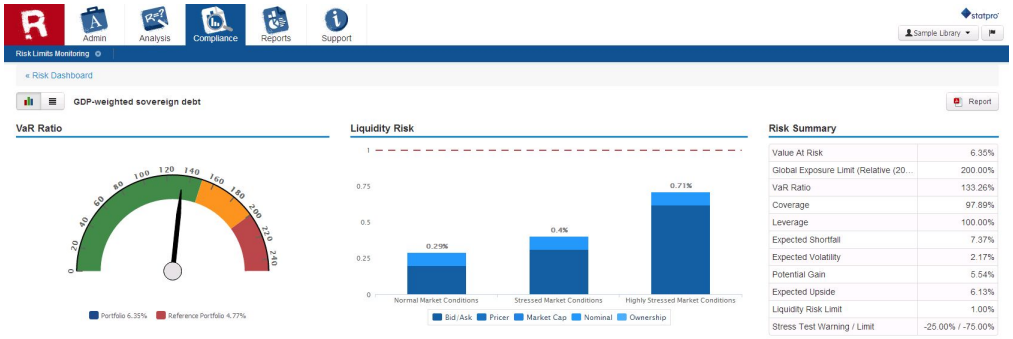
Mini Case-Study

Asset	Vulnerabilities	Risk	POA&M or Risk Treatment
UBHub	- Too much access	Medium	- Restriction of Users (Least Privilege Principle) - Within a year
	- No Documentation - Lack of Knowledge	Medium	- Documentation - Encryption - With two years
	- Misconfigured	High	- Reconfiguration and Documentation with screenshots - Contact Consultants - Within 6 months

*Ownership of Assets

Monitoring Risk

- Yearly reviews/audits
- Change in policies
- New risk assessment criterias
- Change in criminal landscape
- Risk Dashboards



Mini Case-Study

Asset	Vulnerabilities	Risk	POA&M or Risk Treatment	Yearly Check
UBHub	- Too much access	Medium	- Restriction of Users (Least Privilege Principle) - Within a year	- No changes occurred, Possible DATO needed
	- No Documentation - Lack of Knowledge	Medium	- Documentation - Encryption - With two years	- Encryption is in testing environment
	- Misconfigured	High	- Reconfiguration and Documentation with screenshots - Contact Consultants - Within 6 months	- Configured properly, Risk Mitigated

Information and Data | Handling and Classification

- At Rest
- In Transit
- Disposal
- Hard Copy
- Electrical Format
- Storage Media

- Public
- Internal
- Departmental
- Confidential/Sensitive
- Highly Restricted

- **Need to Know**
- **Least Privilege**

Security Frameworks

- COBIT
- ISO 27000 Series
  - 27001
- NIST SP 800 Series
  - NIST 800-53

Compliance

- HIPAA
- FERPA
- PCI-DSS
- FISMA
- State Laws
- International Laws

Risk Management - Summarized

- Planning!
  - Scope, Boundaries
- Asset Management
- Threat Identification
- Vulnerability Identification
  - Auditing and Reviews
- Risk Assessment
  - Asset Risk Level
  - Threat Risks
  - Vulnerability Risks
- Risk Treatment or Risk Response
- Monitoring
- Security Framework
- Compliance
- Info Handling and Classifications

- Compliance
- Security Frameworks
- Planning
- Asset Management
- Threat Identification
- Risk Assessment
- Vulnerability Identifications
- Risk Treatment & Governance
- Monitoring

- https://www.nist.gov/cyberframework