TAC 202/ NIST 800-53 Risk Assessment: The University of Texas at Austin

Drew Scheifele, PhD
Co-Founder, SaltyCloud

Cam Beasley, CISSP
CISO, UT Austin

TEXAS
The University of Texas at Austin

salty cloud

Situation:

Hackers steal Social Security numbers from UT database

ı, Wednesday, March 5, 2003

University breach exposes data on 197,000 people

University of Texas at Austin falls victim to network security breach.

- Two disclosed breaches in three years, escalating impact:
  - Limited visibility into what data was on what systems, and how controlled
  - No ability to measure and document risk over time
  - Limited ability to prioritize resources to improve risk/ enhance security posture

Challenges:

- New CISO/ New comprehensive security policy (2005):
  - Including: Data Classification Standard, Asset Inventory, System Classification, Conduct/ document Risk Assessment

- Challenges with distributed security management, language and controls

- Challenging discussions with board regarding ability to quantify and document risk

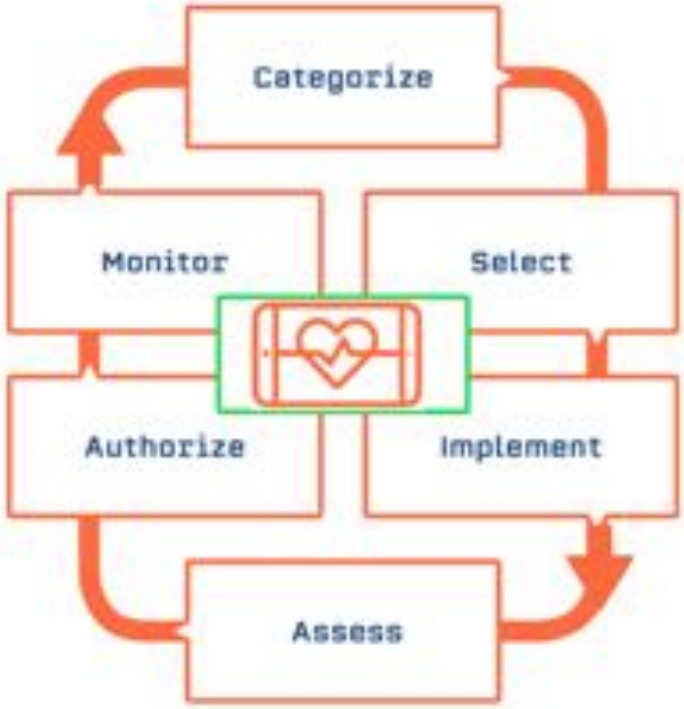
Gap: Search for solution

- Not able to find suitable IT solution suited for EDU space:
  - Integration of data classification standard, system inventory/ classification, and risk assessment
  - Unlimited delegation of question(s) to end user in highly distributed/ federated environment
  - Ability to roll up information by dept/ question set to document/ measure risk over

- Choices:
  - Spreadsheets + Low function survey tools
  - Heavy/ slow on-prep deployments of legacy ASP apps

- Challenging usability and actionability upon completion

Information Security Office Risk Assessment (ISORA)



Two Step Risk Management Solution:

- Inventory and Categorize Systems
  - LDAP/AD integration and API
  - Manual Load
- Campus-Wide/ Focused Risk Assessments
  - Unlimited delegation
  - Roll up by group/ team
  - Reporting by unit or Risk Category

RMP Adapted from NIST 800-37

Improved Risk Profile Driven Through ISORA Include

- Disaster Recovery Plans
  - Increased from 60% to 83% in three years
- Laptop Encryptions
  - Increased from 12-20% to pretty much 100% in three years
- Other areas of significant improvement include:
  - Documentation, IAM, Acquisition Process (procurement), and Disposal

Future Development Roadmap

- Community function to facilitate sharing of question sets and/or Risk benchmarking
- Integration of Application Registry functionality
- Integration of Vulnerabilities, Threat and Incident Data

TAC 202/ NIST 800-53 Risk Assessment at UT Austin

Information Security Office – Risk Assessment (ISORA)

Cam Beasley, CISSP
CISO, UT Austin

TEXAS
The University of Texas at Austin

Classify Assets Individually or In Groups

Export to classify offline

Step 1 Annual Risk Assessment - Info Security Office

Download all hosts as CSV

Info	Tools	Category	Confidentiality / Integrity / Availability	Health / Financial / FERPA	SSN / Research / Critical UT	Critical Department	Save All / Lock All
utmss-master1		Category 1	Confidentiality	Health	SSN	Critical Department	Lock
129.116.116.230			Integrity	Financial	Research	Other:	
24:6E:96:07:A6:48 (Dell Inc.)			Availability	FERPA	Critical UT		
utmss-master2		Category 1	Confidentiality	Health			
129.116.116.231			Integrity	Financial			
24:6E:96:07:89:00 (Dell Inc.)			Availability	FERPA			
utmss-search1		Category 1	Confidentiality	Health			
129.116.116.232			Integrity	Financial			
24:6E:96:08:65:F8 (Dell Inc.)			Availability	FERPA			
utmss-search2		Category 1	Confidentiality	Health			

Modify Hostname Filter

Filtering On

Hide Answered

Hide Unanswered

Hide Locked

Search Across All Surveys

Hide Hosts With Delegates

Sort By IP

Apply Filter Clear Filter Save Filter

scanner

laptop

Filter to classify by type or in bulk

Asset Metadata Fields for Asset Inventory and Classifications

Building: Building... | Room: SZB 518J | Off-premises

Inventory Tag: Inventory Tag...

Serial: Serial...

System: 2

Category: confidential

Categorization: Health, FERPA, Financial, SSN, Research, Critical to Unit, Critical to Organization

Priority: Unknown

System Type: Unknown / Other

Encrypted

Free Fields: []

use the following format: [{"name": "First Field Name", "value": "First Field Value"}, {"
"value": "Second Field Value"}]

Users: Users...

separate multiple values using a comma (Ex. "username1,username2")

IT Contacts: cutronej,br8kaway,felipe,laiey,cpryce,jrk724,jnl583

Risk Assessment Wizard for Non-Technical Respondents

ISO Risk Assessment App | Help | Admin | Super Admin | Logout

Risk Assesssment Wizard

Welcome to the wizard.

Please answer the questions that follow to the best of your ability.

The wizard will help you determine what data classification should be associated with the following system:

Name: security-scanner516.infosec.utexas.edu

MAC: 005056[illegible]69A4

Location: CRBDatacenter

Description: ;IP Address: 146.6.15.60

Click here to continue

Upload, Create, Manage Question Sets for Assessments

isora orgs inventory assessment reports admin logout

ISORA

assessing the enterprise

Assessment Types

	disabled	name
	no	Daryl's Assessment
	yes	Sean's Assessment
	no	Internal Audit - Change in Management
	no	FISMA
	no	NIST 800-53 rev4
	no	PCI DSS v3.1
	no	HIPAA / HITECH
	no	Demo
	no	Shadow Assessment
	no	Portable Device Security
	no	Annual Campus-Wide Risk Assessment

add a new assessment type

name

save

View/ Manage Assessments – Admin Home

ISO Risk Assessment App

Help Admin Super Admin Logout

Your Ongoing Assessments

Reports

Risk Assessment Reports

Security Posture Summaries

Incident Reports

Info Security Office (NFS)

Survey series	ISORA Demo [Edu]
Lead TSC	Cameron D Beasley
Dept Head	Cameron D Beasley
TSCs	22
Delegates	15
Step 1	98 / 196 completed (2 for Lead TSC)
Step 2	445 / 449 completed

Step 1 In Progress - due Wed, Jan 01, 2020

Step 2 In Progress - due Wed, Jan 01, 2020

Refresh survey

(As a precaution, please allow a half hour to pass after updating NetContacts before attempting to refresh the survey).

Launched

Info Security Office (NFS)

Survey series	ALL QUESTIONS WUAHAHA
Lead TSC	Cameron D Beasley
Dept Head	Cameron D Beasley
TSCs	None
Delegates	None
Step 1	0 / 0 completed

Step 1 In Progress - due Wed, Jan 01, 2020

Step 2 In Progress - due Wed, Jan 01, 2020

Refresh survey

(As a precaution, please allow a half hour to pass after updating NetContacts before attempting to

Questions by Category with Parent/ Child Relationships, Conditional, Tags, Partial Credit, etc

ISO Risk Assessment App

Help Admin Super Admin Logout

Step 2 Annual Risk Assessment - Info Security Office

Download all questions as CSV

Department Level Questions 430 / 430 remaining

Save All | Lock All | Expand All | Collapse All

Audit Trails

Are audit logs routinely reviewed?	Unanswered		Lock
Do you restrict access to real time system or audit logs?	Unanswered	thanks	Lock
Do you retain off-line audit logs for a period of time and strictly control access to them?			Lock

Unanswered
Not Applicable
No
Partial (1-33%)
Partial (34-66%)
Partial (67-99%)
Yes

BCP/DRP

Do you maintain system and application documentation at an off-site location?	Unanswered		Lock
Do you routinely verify backups of critical data?	Unanswered		Lock
Have you identified all critical or sensitive services and their upstream/downstream dependencies?	Yes	comment	Lock
Does your Disaster Recovery Plan cover all sensitive and/or critical services?	Yes	all critical ISO services associated with Incident Handling and Response are covered in the Restarting Texas service.	Lock
Does the Disaster Recovery Plan identify the location of stored backups?	Yes		Lock
Has the Disaster Recovery Plan been approved by key affected parties?	Unanswered		Lock

Risk Scores Compared to Campus Average

Risk Score by Categories/ Families

Category Drill Down (popups)

Score breakdown by risk category (View all responses)

The following is a breakdown of this department's risk score (86.9%) by risk category. This breakdown shows the scores by category for the current and previous year's surveys. A trend line for the last several years is also provided.

Risk Category Data	Current Survey	Previous Survey	Trend (Years)
Audit Trails	100.0%	100.0%	
BCP/DRP	55.6%	54.5%	
Development/Acquisition/Design Phase	100.0%	100.0%	
Disposal Phase	100.0%	100.0%	
Documentation	100.0%	100.0%	
Identification and Authentication	61.1%	61.1%	
Implementation Phase	100.0%	100.0%	
Incident Management	100.0%	100.0%	
Logical Access Controls	86.3%	86.3%	
Monitoring and Logging	100.0%	100.0	
Operations/Maintenance Phase	100.0%	100.0	
Personnel Security	100.0%	100.0	
Physical Access Control	100.0%	100.0	
Portable Device Security Report	100.0%	Not pr	
Review of Security Controls	100.0%	100.0	
Security Awareness, Training, and Education	100.0%	75.0%	

Answers breakdown by category: Disposal Phase (Download as CSV)

Dept Code	Question	Answer	Score Actual/Possible	Comment
ACES	[59] Do you purge, overwrite, degauss, or destroy all Confidential information or media when it's disposed of, sent to surplus, or used elsewhere?	Y	7 / 7	No comment
ACES	[65] Do you shred or destroy all hardcopy media with Confidential data when it's no longer needed?	Y	7 / 7	No comment
ACES	[64] Do you securely store or destroy (via the campus media destruction service) all damaged media containing Confidential data?	Y	7 / 7	No comment

	Total Questions	Total Yes	Total No	Total Partial	Total N/A	Merit Points	Improvement Points	Score	Max Score	Percent
ACES	3	3	0	0	0	0	0	21	21	100.0%

ACTS	[59] Do you purge, overwrite, degauss, or destroy all Confidential information or media when it's disposed of, sent to surplus, or used elsewhere?	Y	7 / 7	No comment
ACTS	[65] Do you shred or destroy all hardcopy media with Confidential data when it's no longer needed?	Y	7 / 7	No comment
ACTS	[64] Do you securely store or	Y	7 / 7	No comment

Answers breakdown by category: Logical Access Controls (Download as CSV)

Question	Answer	Score Actual/Possible	Comment
[249] Are firewalls or secure gateways installed? (This includes host-based firewalls.)	Y	5 / 5	No comment
[308] Do you have any enterprise firewalls or secure gateways that are not rest locked?	N	0 / 0	No comment
[161] Do you use file or disk encryption services to protect all data stored on laptops, desktops, portable devices, and removable media?	Y	5 / 5	No comment
[163] Does ITS provide and manage all encryption services your department uses (Digital Certificates, SecureDoc, GPG)?	Y	7 / 7	No comment
[172] Are all Confidential data transmissions requiring confidentiality encrypted? For more information on sensitive data, see Data Classification Standard.	Y	7 / 7	No comment

Summary

Total Questions	Total Yes	Total No	Total Partial	Total N/A	Merit Points	Improvement Points	Score	Max Score	Percent
5	4	1	0	0	20	7	14	21	66.3%

About

This view provides a breakdown of a department's answers for a specific question category.

Important! This view provides statistics and answers for a single department only – no subdepartment answers are taken into account!

Note that questions may be unanswered for one of three reasons:

- Failure to answer a question
- Question is a child of another question which was answered unfavorably
- Question is a child of another question which was answered as not applicable

For more information on how scores are calculated, see the methodology page.

TAC 202/ NIST 800-53 Risk Assessment: The University of Texas at Austin

Cam Beasley, CISSP
CISO, UT Austin

cam@utexas.edu

Drew Scheifele, PhD
Co-Founder, SaltyCloud

drew@saltycloud.com