METRO STATE UNIVERSITY

CAE IN CYBERSECURITY COMMUNITY

Cybersecurity Clinic

Faisal Kaleem

APRIL 16, 2024

Metro State University

- An NSA designated Center of Academic Excellence in Cyber Defense Education (NCAE-CD).

NSA-designated CAE-CD Institution

- A **Beyond the Yellow Ribbon University**, serving the most veterans and active-duty military members in the Minnesota State System.
- Ranked **#22 in the nation** and **#1 in Minnesota** for promoting the social and economic mobility of its graduates (CollegeNet-2022)
- Cybersecurity Bachelor's program ranked **#2 Most Affordable** and **#7 Best Overall** (Cybersecurity Guide's 2024 rankings)

MN Cyber

- A statewide public-private partnership for cybersecurity education, research, and training
- The main goal is to position Minnesota as a national leader in cybersecurity and its related workforce through education, legislative and community engagement, and innovative public-private partnerships.
- Advisory Board members include
  - CISOs from major twin-cities organizations, including MN.IT
  - National Guards
  - State Legislators

MN CYBER

Train. Test. Detect. Protect.

What is a Cybersecurity Clinic?

- A student-centered program that offers a range of cybersecurity-related services to various organizations and communities
- An innovative approach that addresses the dual challenges of educating future cybersecurity professionals and fortifying cybersecurity resilience in vulnerable communities.
  - The aim is to improve the client's cybersecurity awareness, readiness, and resilience while providing experiential learning opportunities to students (and a possible pathway for employment)
- **More Information:** Clinic Consortium Website
  - https://cybersecurityclinics.org/

Cybersecurity Clinic Goals

- **Broadening:** Experience broader aspects of cybersecurity
- **Deepening:** Gain a deeper understanding of the digital safety needs and challenges for under-resourced civil society
- **Hands-on:** Gain hands-on experience uncovering practical solutions to those cybersecurity challenges
- **Impact:** Create positive change in the real world by protecting civil society

Metro's Cybersecurity Clinic

- NSA-sponsored two years project with an optional third year
- **Pilot Phase:** Being offered as a Semester long Capstone/Internship Experience
- Involved both Undergraduate and Graduate Students
  - Students come with diverse backgrounds and academic expertise
- **A collaborative effort**: Academia and State IT (MN.IT)
  - Exploring the unique synergy between academia and state IT
  - Providing an environment for students where theoretical knowledge meets practical application

Metro's Cybersecurity Clinic

- Provides free cybersecurity risk assessments to underprivileged sectors, including K12 institutions, underserved municipalities, non-profits, and small businesses
- Clients' Risk Assessment Sessions are either in-person or virtual (if the client is far away) and based on CIS IG1 controls
  - https://www.cisecurity.org/controls/implementation-groups/ig1
- Faculty Member and MN.IT staff attend sessions as observers, gauge student team's performance, and provide feedback
- Students must attend a Pre-Assessment meeting for every client

Metro's Cybersecurity Clinic

- Students collect the client responses into an Excel Sheet and then compile the data into a comprehensive report
- The report is vetted by both Metro's faculty and MN.IT before it is handover to the client
- Students make a final presentation and submit the final report to fulfill their academic requirements

Services Included

- **Level 1:** Comprehensive Risk Assessment
  - May also include Cyber Hygiene/Awareness Training, Security Controls recommendation, and Policy Development
- **Level 2:** Vulnerability Assessment, Penetration Testing, IR Plans, CMMC Certifications
- **Level 3:** Day-to-day security incident monitoring in the Security Operations Triage Center
  - Provides low-cost subscription-based services
  - Provides Cyber Residency for students
- Levels 2 and 3 are planned for next iteration

Participation Requirements

- Students must be at least at a Junior Level in the Cybersecurity major with a 3.0 CGPA
- Must be US Citizens or Permanent Residents
- Must work in a Team led by a Graduate Student
- Must have completed the following:
  - Pass the CompTIA Security+ Certification
  - MIT's Cybersecurity for Critical Urban Infrastructure online course
- Must have attended Mock Training Sessions
- Must be familiar with CIS IG1 controls
- Must have read and signed various Agreements
- Participants can continue beyond one semester after fulfilling additional requirements

Client Recruitment

- MN.IT is responsible for Public K12 Schools, Counties/Cities, and Non-Profits
  - 500+ requests have already been received for providing assessment services
  - This includes various public K12 schools, Counties and Cities, and small utility companies (Critical Infrastructure Sector)
- Metro State is responsible for SMBs
  - Leveraging SBA and various Chamber of Commerce to reach out to SMBs
  - A few requests have been received to provide a free assessment
  - During the pilot phase, we are mainly focusing on clients other than SMBs
  - Next iteration will include risk assessments for SMBs

Resources Developed

- Risk Assessment Scoring Excel Sheet based on CIS Controls IG1 group
- Risk Assessment Report Template
- A Workbook to help guide students on how to use the Scoring sheet
- Rubrics to gauge student performance and participation
- Procedure to guide the supervisory group to review reports
  - Supervisory group comprises Metro's Faculty and MN.IT staff

Cyber Risk Register

Enterprise Risk Assessment Criteria	
Enterprise Name	
Respondent Name	
Respondent Email	
Last Completed (Date)	

Risk Register	Risk Analysis				Risk Treatment	
CIS Safeguard #	CIS Safeguard Title	NIST CSF Security Function	Asset Class	Safeguard Maturity Score	Risk Treatment Safeguard Description	Notes
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Identify	Devices		Establish and maintain an accurate, detailed, and up-to-date inventory of all Enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, Enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the Enterprise's network infrastructure, even if they are not under control of the Enterprise. Review and update the inventory of all Enterprise assets bi-annually, or more frequently.	
1.2	Address Unauthorized Assets	Respond	Devices		Ensure that a process exists to address unauthorized assets on a weekly basis. The Enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	
2.1	Establish and Maintain a Software Inventory	Identify	Applications	1	Establish and maintain a detailed inventory of all licensed software installed on Enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	
2.2	Ensure Authorized Software is Currently	Identify	Applications		Ensure that only currently supported software is designated as authorized in the software inventory for Enterprise assets. If software is unsupported, yet necessary for the fulfillment of the Enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported	

Risk Register | Legend | Lookup Tables | Bar Chart

Risk Register (Legends)

Color Key		Automated or fixed values on the Risk Analysis side of the Risk Register. While the worksheet is in protected mode, these values cannot be changed.
		Automated or fixed values on the Risk Treatment side of the Risk Register. While the worksheet is in protected mode, these values cannot be changed.
		For user input. Risk assessors will add values into these columns.
		For optional user input. Risk assessors may add values into these columns if it's useful to them.
		Automated or fixed values on the Reasonable Annual Cost side of the Risk Register. While the worksheet is in protected mode, these values cannot be changed.

	Title	Meaning
Risk Analysis	CIS Safeguard #	The unique CIS Safeguard identifier, as published in the CIS Controls.
	CIS Safeguard Title	The title of the CIS Safeguard, as published in the CIS Controls.
	NIST CSF Security Function	Mapping between the NIST CSF Security Functions and CIS Safeguards, as published in the CIS Controls.
	Asset Class	The asset class, as published in the CIS Controls.
	Safeguard Maturity Score	A score of '1' through '5' designating the reliability of a Safeguard's effectiveness against threats.
	VCDB Index	An automatically calculated value to represent how common the related threat is as a cause for reported cybersecurity incidents.
	Expectancy Score	An automatically calculated value to represent how commonly the related threat would be the cause of a cybersecurity incident, given your current Safeguard.
	Impact to Mission	The magnitude of harm that a successful threat would cause to your Mission.
	Impact to Operational Objectives	The magnitude of harm that a successful threat would cause to your Operational Objectives.
	Impact to Obligations	The magnitude of harm that a successful threat would cause to your Obligations.
	Risk Score	The product of the Expectancy and the highest of the three Impacts.
	Risk Level	An evaluation of the risk as acceptable, unacceptable, or catastrophic.
	Risk Treatment Option	A statement about whether the enterprise will accept or reduce the risk.
	Risk Treatment Safeguard	The unique CIS Safeguard identifier, as published in the CIS Controls.
	Risk Treatment Safeguard Title	The title of the CIS Safeguard, as published in the CIS Controls.
	Risk Treatment Safeguard Description	The description of the CIS Safeguard, as published in the CIS Controls.

Impact Scores	Mission	Operational Objectives	Financial Objectives	Obligations
Definition	*Required*	*Required*	*The high dollar limit for each impact score.*	*Required*
1. Acceptable	We would achieve our mission.	We would meet our objectives.	Optional	No harm would come to o
2. Unacceptable	We would have to reinvest or correct the situation to achieve our mission.	We would have to reinvest or correct the situation to achieve our objectives.	Optional	The harm that would com would be correctable.
3. Catastrophic	We would not be able to achieve our mission.	We would not be able to meet our objectives.		The harm that would com would not be correctable.

Inherent Risk Criteria			
Asset Class	Mission Impact	Operational Objectives Impact	Obligations Impact
Enterprise	*Required*	*Required*	*Required*
Devices	Optional	Optional	Optional
Applications	Optional	Optional	Optional
Data	Optional	Optional	Optional
Network	Optional	Optional	Optional
Users	Optional	Optional	Optional

Risk Levels	
Red	Red indicates that the risk is "urgent."
Yellow	Yellow indicates that the risk is "unacceptably high, but not urgent."
Green	Green indicates that the risk evaluates as "acceptable."

Risk Register (Lookup Table)

Maturity Scores	Used for "Safeguard Maturity Score" and "Risk Treatment Safeguard Maturity Score"

Maturity Scores	Definition
1	Safeguard is not implemented or is inconsistently implemented.
2	Safeguard is implemented fully on some assets or partially on all assets.
3	Safeguard is implemented on all assets.
4	Safeguard is tested and inconsistencies are corrected.
5	Safeguard has mechanisms that ensure consistent implementation over time.

Expectancy Criteria	Used for "Expectancy Score" and "Risk Treatment Safeguard Expectancy Score"

Expectancy Scores	Expectancy Definition
1	The risk is not expected in this environment.
2	This risk should be expected to cause a security incident at some time.
3	We should expect this to happen soon, if it has not already occurred.

Risk Acceptance Criteria	Used to evaluate risk acceptance

Acceptable Risk Score	Risk Acceptance Criteria
<6	All scores lower than '6' may be automatically accepted. All other risks must be reduced.

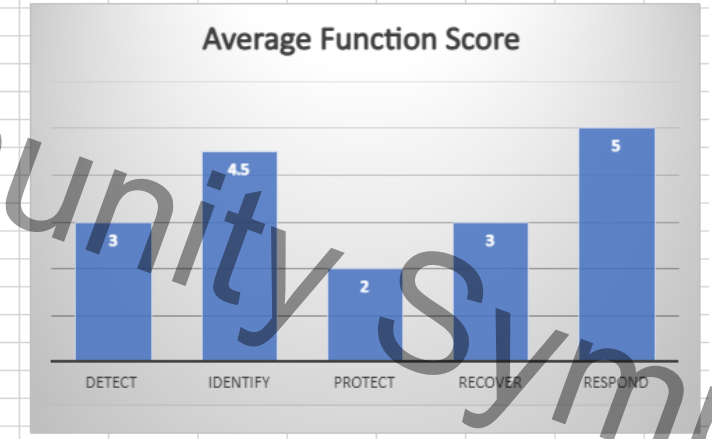
VCDB Index	Used to populate "VCDB Index"

Incident Count	8893	As of	7/29/2021

Asset Class	Sum of Threat Count / Industry	Percentage	Index
Enterprise	4458	50%	3
Applications	1253	14%	2
Data	4458	50%	3
Devices	798	9%	1
Network	62	1%	1

Bar Chart

Security Func	Avg Safeguard Ctrl
Detect	3
Identify	4.5
Protect	2
Recover	3
Respond	5



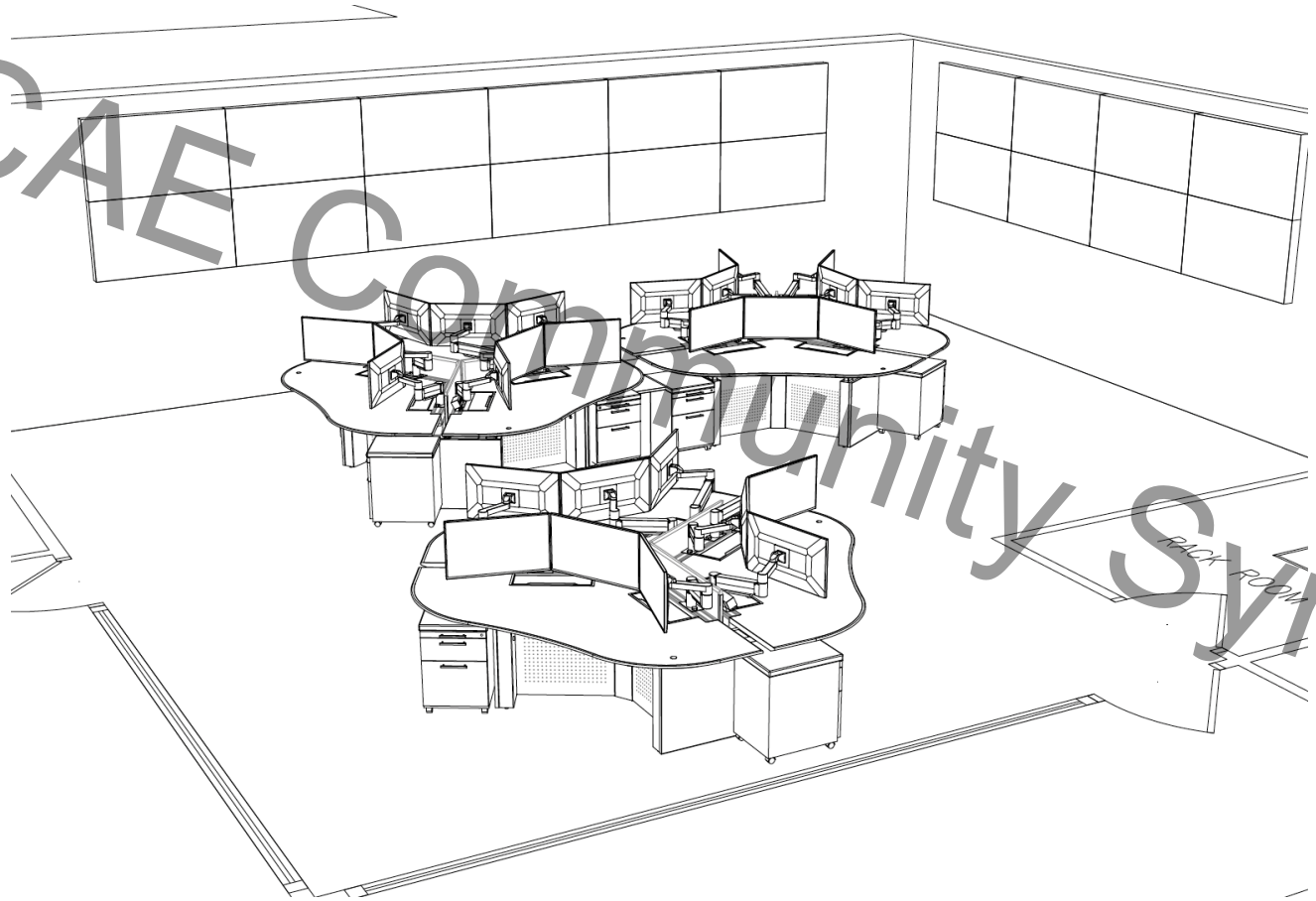
Asset Class	Avg Safeguard Ctrl
Applications	5
Data	3
Devices	3.2
Enterprise	1.6
Network	2.2
Users	4.5

Lessons Learned

- Establishing Credibility With Clients
  - Collaboration with MN.IT helped
- Challenges about operating at scale
  - Most of the cybersecurity clinic deals with a small number of organizations per semester
  - 15+ organizations are being served this semester
- Think about Liability issues
  - Metro State and MN.IT are both state entities, so this was not an issue for our clinic
- Dealing with Client/Student Schedule
- Varying students' preparation and engagement levels
  - Non-traditional students with jobs and other responsibilities pose challenges
  - Had to reorganize the student teams at the last moment
  - A phased approach to launch the teams, work

Cybersecurity Clinic

SOC @ 809 7th Street E



SOC @ 809 7th Street E

Thank You

with a 3.0 CGPA

METRO STATE UNIVERSITY

NSA-designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.