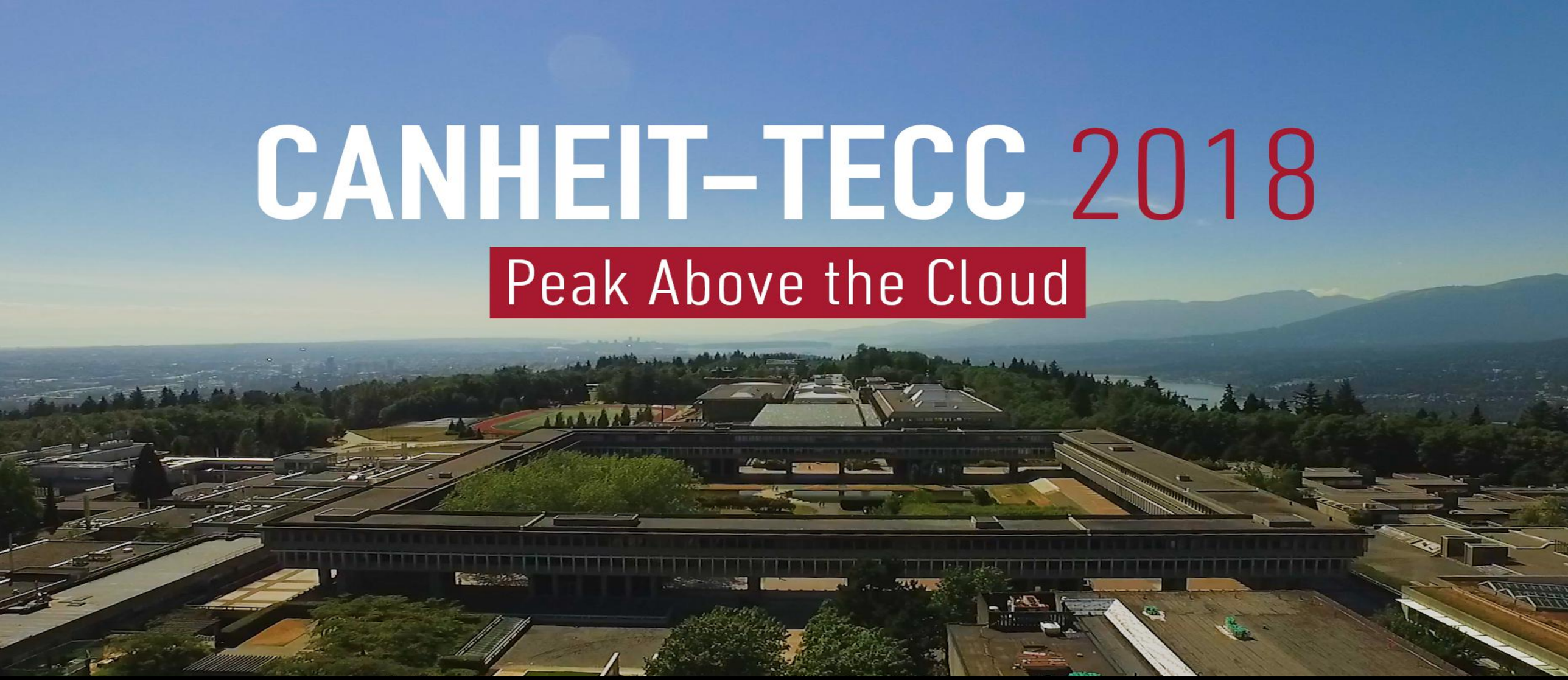


Developing a Model for Cyber Security Maturity Assessment

Tariq Al-idrissi, Associate Vice President IT, Trent University
Ian Thomson, Information Security Officer, Trent University

June 20th, 2018 (8:45am – 9:30am)

MacEwan University defrauded of $11.8M in online phishing scam

Hacker Greenw people's

Student applican

18-year-old facing

CBC News Posted: Nov 2

Student Expelled Change Grades

By Ca

Help Net Security
March 30, 2018

Crypto mining runs rampant in higher education: Is it

Massive cyberhack by Iran allegedly stole research from 320 universities, governments, and companies

By Jon Cohen | Mar. 23, 2018 , 4:15 PM

Nine Iranians working on behalf of the Islamic Revolutionary Guard Corps hacked the computers of 7998 professors at 320 universities around the world over the past 5 years, **an indictment filed by a federal grand jury** alleges. The hackers stole 31.5 terabytes of documents and data, including scientific research, journals, and dissertations, the indictment alleges. Their targets also included the United Nations, 30 U.S. companies, and five U.S. government agencies.

Uni swe

More tha

CBC

December

Stanf staffe

The Unive student ar the last year.

According to a graduate student, the attackers have asked for 39 bitcoin to unlock all of Carle Tessier/Reuters)

sed

University Cyber Facts

"The cyber attacks on education sector has more than doubled in the first six months of 2017 compared to the last half of 2016" - *Gemalto*

Deloitte has identified unique challenges for Universities:

- Limited resources and decentralized IT operations
- Plethora of valuable data
- Minimal cyber security training for staff and students
- Variety of devices used by students and faculty (BYOD)
- Lack of access controls

According to the 2017 **Verizon** data breach report, phishing attacks cause **90%** of cybersecurity breaches.

“If **you can't** measure it, **you can't manage** it.” Peter Drucker

Cyber Security Maturity Measurement

Why Select a Standard?

There is No Such Thing As Perfect Protection

A Good Maturity Program will Help You Access Your Level of Risk Accurately

High Risk
Low Cost

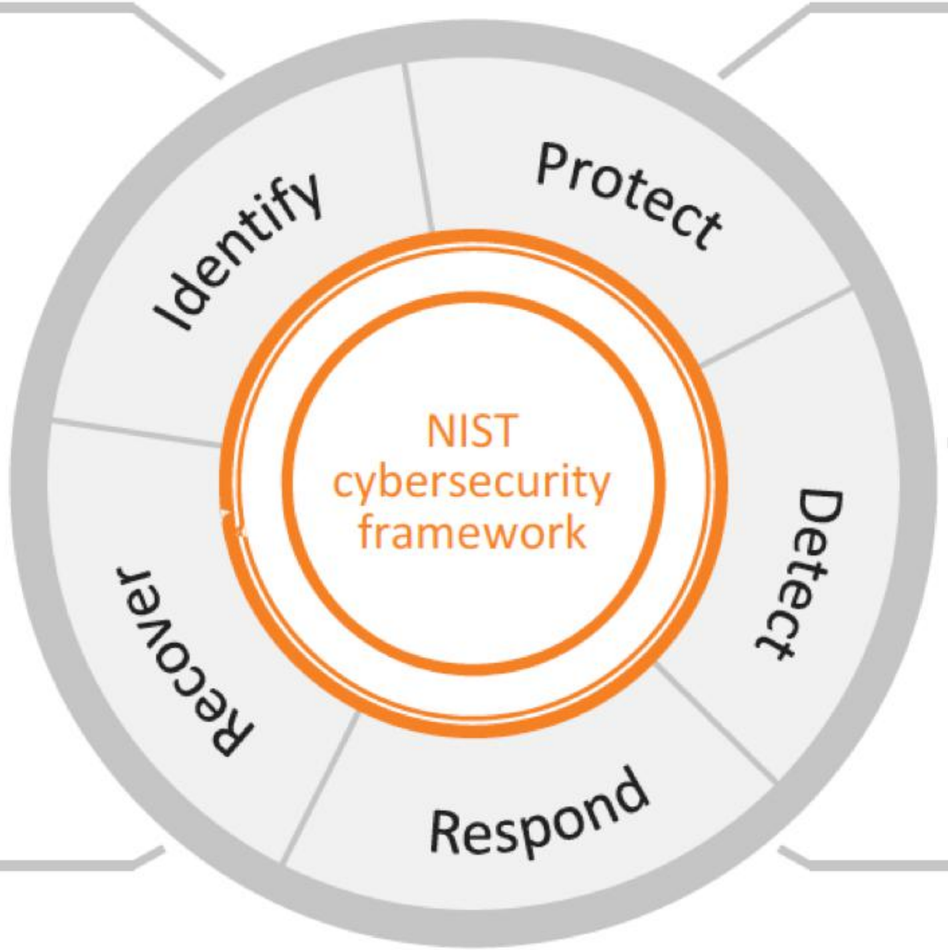
Low Risk
High Cost

You have to Continuosly Reassess How Much Risk is Appropriate

NIST Cyber Security Framework

Identify
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities

Protect
Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services

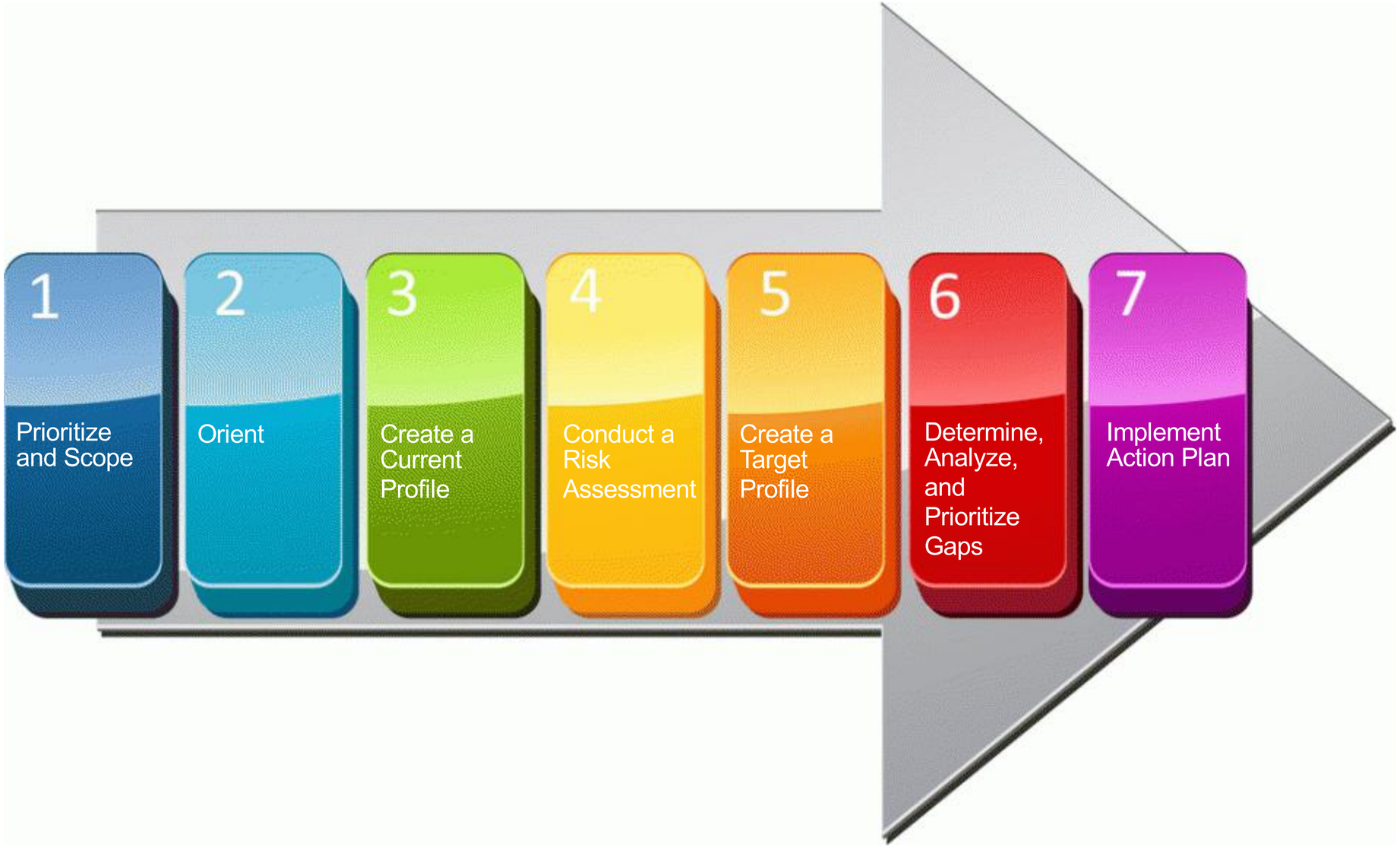


Detect
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

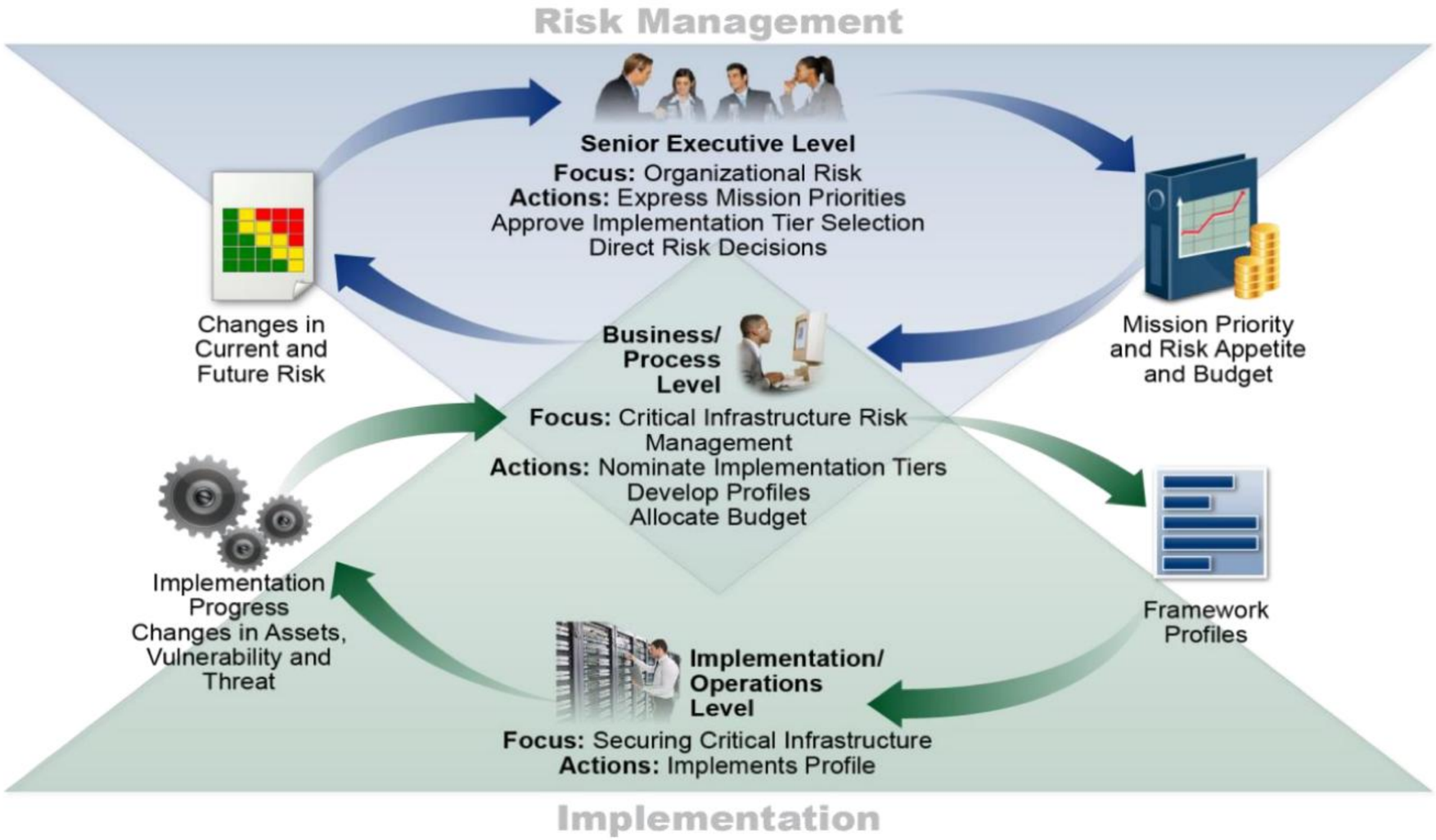
Recover
Develop and implement the activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity event

Respond
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event

Implementation Guidance Through a Seven Step Process

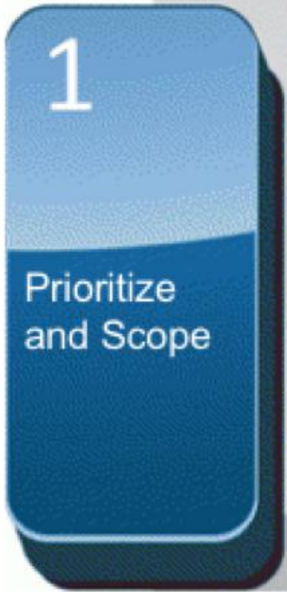


Roles



Source: Framework for Improving Critical Infrastructure Cybersecurity, NIST, USA, 2018, Figure1

Step 1: Prioritize and Scope



High Level Activities of this Step

- Identify key executive and board level stakeholders that authoritatively speak to mission drivers and risk appetite.
- Determine the scope to be addressed through the application of CSF. Is this organizational or partial?
- Identity organizational vision, mission, and strategies/drivers. These will provide an input and alignment into other implementation steps.
- Identify risk architecture.
- Define the roles and responsibilities for conveying prioritization and resource availability.
- Establish a governance steering group that will remain informed on cyber security issues, threats, and mitigation progress.

Step 2: Orient and Step 3: Create a Current Profile

High Level Activities of these Steps

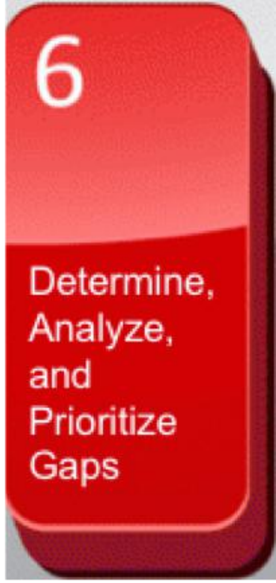
- Organize an operational level governance group.
- Determine business and operational systems on which stakeholder drivers (as described in Phase 1) depend.
- Ascertain availability goals and/or recovery goals for identified systems and assets.
- Review the implementation tiers and record the tier selected by the organization.
- Complete the current profile template iterating through each subcategory and recording status;
    - N: Not Achieved (0 to 15%)
    - P: Partially Achieved (>15 – 50%)
    - L: Largely Achieved (>50 to 85%)
    - F: Fully Achieved (>85%)

Step 4: Conduct a Risk Assessment and Step 5: Create a Target Profile

High Level Activities of these Steps

- Conduct risk assessment to catalog potential risk events to applicable systems and assets
- For each risk event above, determine potential of that risk being realized and the overall impact on the organization. Think about emerging risks, threat, and vulnerability data.
- Determine the applicability of a subcategory for your organization.
- Determine additional categories of subcategories.
- Complete the Target Profile template, iterating through each subcategory and recording desired state. You *need not achieve the highest desired state*.
    - N: Not Achieved (0 to 15%)
    - P: Partially Achieved (>15 – 50%)
    - L: Largely Achieved (>50 to 85%)
    - F: Fully Achieved (>85%)

Step 6: Determine, Analyze, and Prioritize Gaps



High Level Activities of this Step

- For each subcategory listed in the Target Profile, record the difference between the desired capability level and the current state (as described in the current profile).
- Determine required activities for each subcategory to close the gap between current state and target state.
- Review the potential activities defined, determine the appropriate priority of those activities. This is to align with risk appetite.
- Determine the resources necessary to accomplish the activities described.
- Create and record an action plan of activities with milestones, ensuring appropriate responsibility and accountability, to achieve the desired outcomes according to the determined priorities.

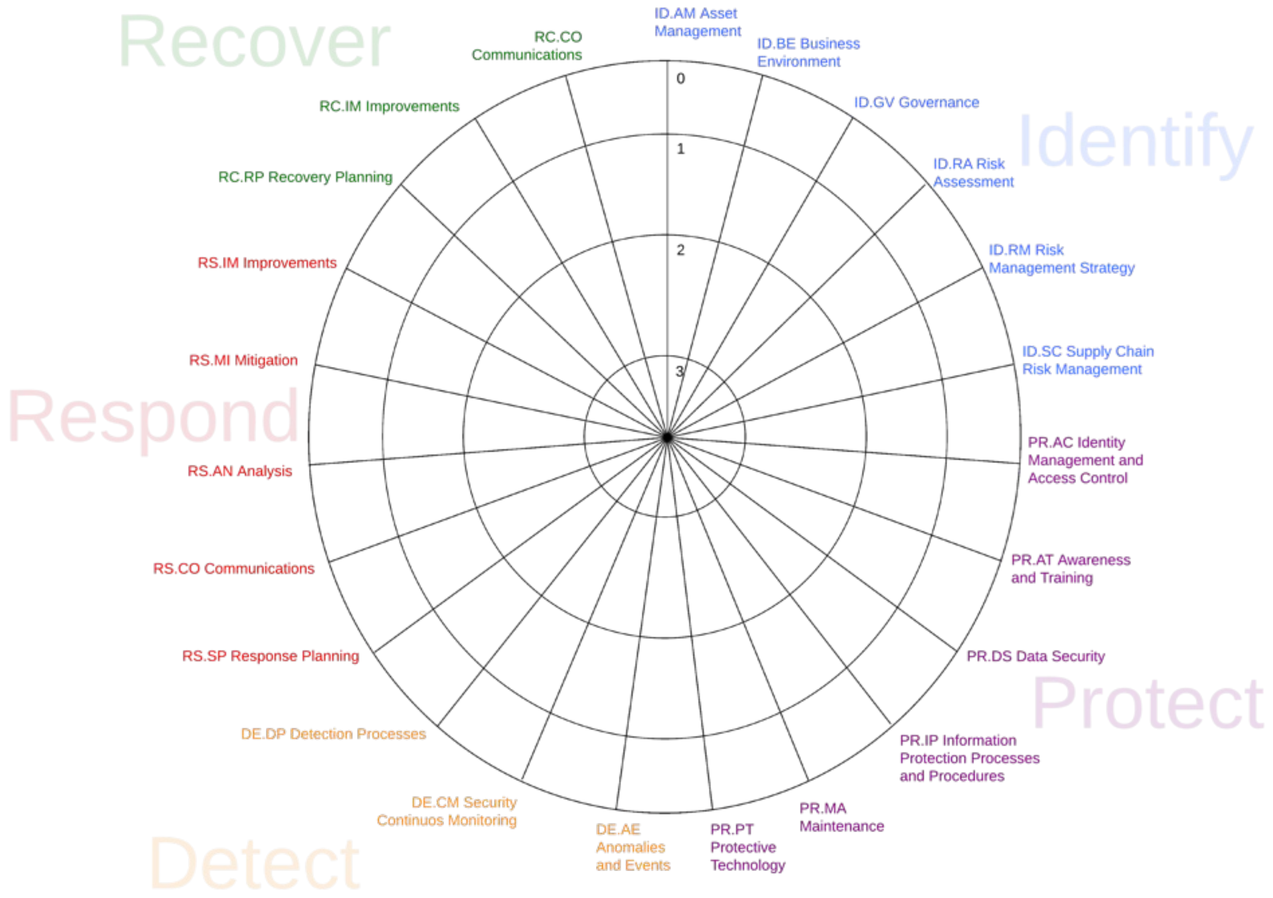
Step 7: Implement Action Plan

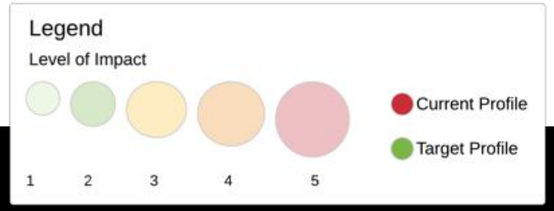
High Level Activities of this Step

- Execute the action plan as defined step 7
- Consider a continuous feedback loop and metrics development to your governance committee
- Assist in the resolution of significant issues
- If necessary, you may need to adjust;
    - The target profile
    - Gap Assessment
    - Action Plan

Cybersecurity Maturity Radar

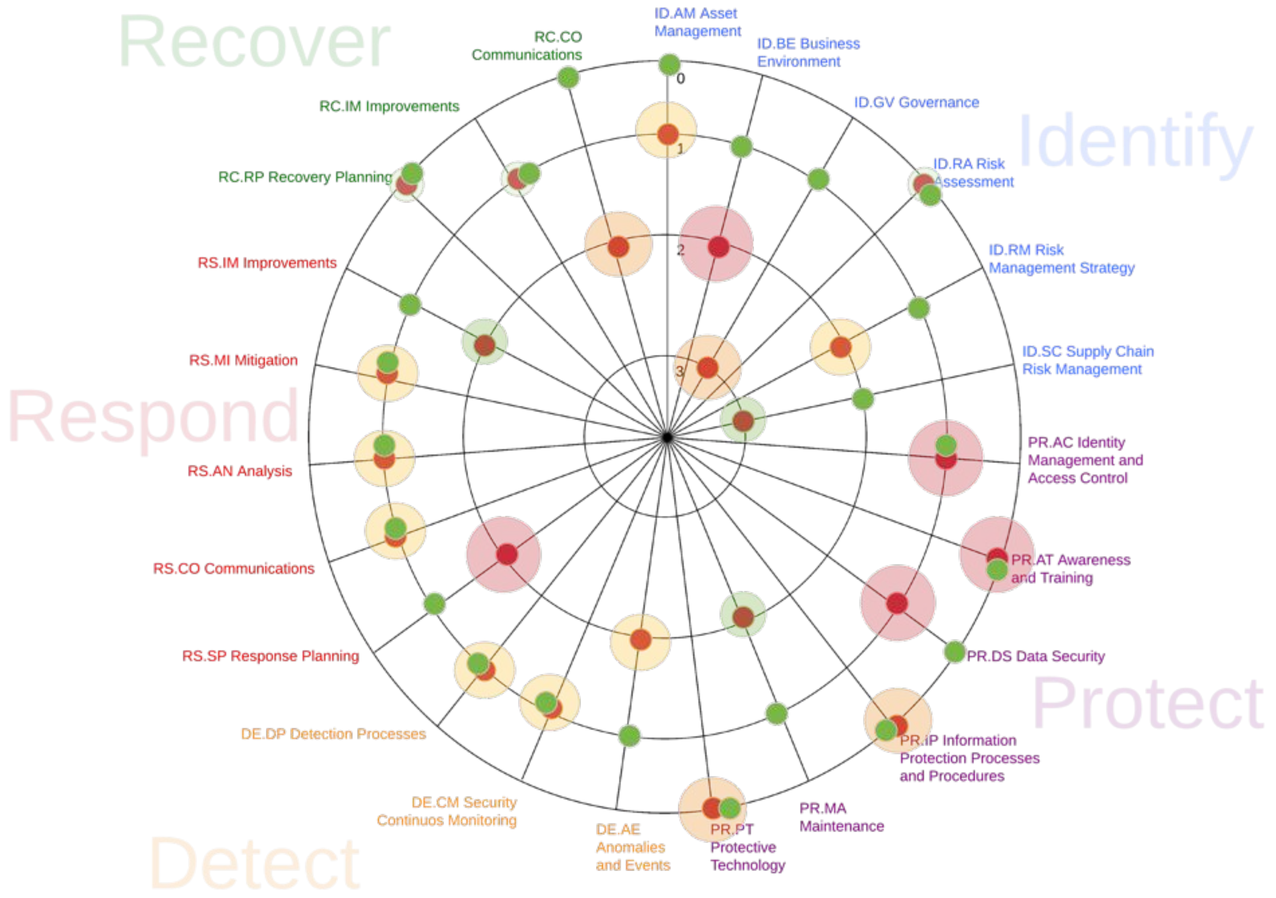
Current Score: XXX Target Score: XXX

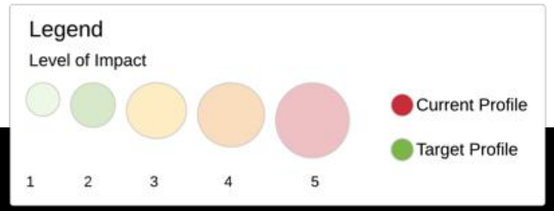




Cybersecurity Maturity Radar

Current Score: 95 Target Score: 53





Cyber Security Assessment Tool - Organization Profile

- Basic Information about organization structure
- Designed to help identify key information about critical systems
- Identify who may be participating in interviews

Roles	
The following roles have been defined by relevant standards. Enter in the space provided the name of the person who best fits that role in your organization.	
Leadership / Executive / Management	
Project Sponsor / Owner	
Chief Information Officer	
Chief Information Security Officer	
Human Resources Manager	
Facilities Manager	
Physical Security Manager	
IT Manager - Networking	
IT Manager - Client Services	
IT Manager - Information Systems	
IT Manager - Project Management	
Legal Department	
Risk and Compliance Officer	
Finance Manager - Audit and Controls	
Technical / Functional	
Information Security Officer	
Security Analyst	
System Administrator / Architect	
System Administrator / Architect	
System Administrator / Architect	
System Administrator / Architect	

A	B
Organization Information	
Organization Name	
Organization Address	
Assessment Executive Sponsor	
Assessment Technical Leader	
Assessment Date	
Assessment Scope	
Critical Systems and Infrastructure	

Cyber Security Assessment Tool - Interview Preparation

- Each subsection of the NIST framework has been divided into an interview with suggestions on those who should be present in the interview

Interview	Roles	Suggested Interview Time
Management Processes, Governence and Compliance	Chief Information Officer Chief Information Security Officer Legal Department Risk and Compliance Officer Finance Manager - Audit and Controls Information Security Officer	1 Hour
Business Operations and Business Processes	IT Manager - Client Services IT Manager - Information Systems IT Manager - Project Management Risk and Compliance Officer Finance Manager - Audit and Controls Information Security Officer Security Analyst Programmer Programmer	1 Hour
Security Operations	Chief Information Security Officer IT Manager - Networking Information Security Officer Security Analyst Service Desk Analyst	1 Hour

Cyber Security Assessment Tool – Assessing Current State

- Each subsection has been divided into an interview
- Conduct the interview and attempt to quantify the response to the question and the objectives
- Spectrum from 0.00 to 1.00 can be used for score
- Score is a rough guide only, project team will review all sub categories later
- Some subcategories have multiple questions

Subcategory	Objectives	Question / Evidence	Score /1	Comments
ID.GV-1: Organizational information security policy is established	A clearly defined and executive supported information security policy	Does you organization have an information security policy or policies that are supported by senior management?		
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Clearly defined accountability, roles and responsibilities for cyber-security focused individuals	Do job descriptions and management portfolios contain clear responsibility and accountability for information and cybersecurity?		
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	The organization is in compliance with relevant legal and regulatory regulations. Regulations that are relevant to the organization are widely understood and processes are in place to manage compliance	Does your organization comply with relevant legal and regulatory standards (PCI-DSS, PIPEDA, etc..)		
		Do cyber security policies present in your organization map to relevant legal and regulatory standards?		
		Do you regularly perform audits do ensure your compliance with legal and regulatory standards?		

Cyber Security Assessment Tool – Assessing Current State

- Each subcategory is automatically scored based on the criteria mentioned in previous slides
- After each category has been scored the project team can review the derived score to ensure the tool is generating useful data for the institution

Category	Subcategory	NIST Testing Steps	Interview Score /100	Score	Relevant COBIT Practices
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	1. Obtain a copy of the organization's logical network diagram (LND), data flow diagrams, and other network and communications diagrams. 2. Review the diagrams for the following: a. Frequency of updates to diagrams b. Accuracy and completeness of diagrams c. Scope of diagrams is adequate to identify both domains of different risk and control levels (i.e., high-risk, publicly-accessible portions of a network vs. high-value, restricted access portions of the network) and the control points (e.g., firewalls, routers, intrusion detection/prevention systems) between them. 2. Determine if tools (e.g., security event and information management systems [SIEMs]) are used to establish typical (baseline) traffic so abnormal traffic can be detected.	0	N: Not Achieved (0 to 15%)	DSS03.01
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	1. Obtain a copy of policies and procedures regarding system and network monitoring. a. Determine if policies and procedures require monitoring for anomalous activity at identified control points. 2. Obtain a copy of detected events (e.g., alerts from IDS) and the organization's response to them. Review the events and responses to ensure thorough analysis of detected events is performed.	0	N: Not Achieved (0 to 15%) P: Partially Achieved (>15 – 50%) L: Largely Achieved (>50 to 85%) F: Fully Achieved (>85%)	
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	1. Obtain a listing of event aggregation and monitoring systems in use at the organization (e.g., SIEMs, event log correlation systems). 2. Obtain a list of sources that provide data to each event aggregation and monitoring system (e.g., firewalls, routers, servers). 3. Compare the sources to identified control points between domains of different risk and control levels and determine if they provide adequate monitoring coverage of the organization's environment.	0	N: Not Achieved (0 to 15%)	
	DE.AE-4: Impact of events is determined	1. Obtain a copy of detected events and the organization's responses to them. 2. Review the events, tickets and responses in order to ensure the organization is documenting the impact of anomalous activity using metrics that are applicable to the organization (e.g., compliance impact, operational impact, accurate reporting impact).	0	N: Not Achieved (0 to 15%)	APO12.06

Cyber Security Assessment Tool - Current Profile Summary

- Based on the information recorded in the interview and on the summary sheets a current profile summary sheet is displayed that outlines where the institution currently sits relative to the NIST sub categories
- This page shows all subcategories except those fully achieved.

Identify		
Subcateogry	**Score**	**Interview Score /100**
ID.AM-1: Physical devices and systems within the organization are inventoried	**N: Not Achieved (0 to 15%)**	0
ID.AM-2: Software platforms and applications within the organization are inventoried	**N: Not Achieved (0 to 15%)**	0
ID.AM-3: Organizational communication and data flows are mapped	**N: Not Achieved (0 to 15%)**	0
ID.AM-4: External information systems are catalogued	**N: Not Achieved (0 to 15%)**	0
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**N: Not Achieved (0 to 15%)**	0
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**N: Not Achieved (0 to 15%)**	0
ID.BE-1: The organization's role in the supply chain is identified and communicated	**N: Not Achieved (0 to 15%)**	0
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**N: Not Achieved (0 to 15%)**	0
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**N: Not Achieved (0 to 15%)**	0
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**N: Not Achieved (0 to 15%)**	0

Cyber Security Assessment Tool - Threat Assessment

- The threat assessment page allows the instruction to consider threats to the critical infrastructure that has been identified in the organizational profile.
- This data is used in the risk assessment for each NIST subcategory and helps to determine the importance of the threat and eventually the control categories.

Threat	Impact of Threat 1 = Little Impact 5 = High Impact	Liklihood of Threat 1 = Not Likely 5 = Very Likely	Risk Score	Risk Quotient
DDoS by Student	5	5	25	High
DDoS by External Party			0	Low
Advanced Persistent Threat Attack			0	Low
Phishing Message Targeting Credentials			0	Low
			0	Low
			0	Low
			0	Low
			0	Low
			0	Low
			0	Low
			0	Low
			0	Low

1
2
3
4
5

Examine the threat landscape your institution faces relative to the critical systems you identified earler. For each threat, extrapolate the Impact and Liklihood of the threat being exploited

System Name	System Priority
ERP - Student Information System	5

Cyber Security Assessment Tool – Risk Assessment

- After reviewing the current assessment and determining threats for the institution, the project team then completes a risk assessment for each of the NIST sub categories. Essentially trying to answer the question “What is the impact of not having this control in place”
- This information should be gathered relative to the threats to critical infrastructure that were identified in the target profile.
- This information helps to determine if the NIST guidelines are relevant to the institution as depending on institutional size and scope they may not be.

Cyber Security Assessment Tool - Risk Assessment

Identify	Current Profile Score	Impact of not having control in place 1 = Low Impact 5 = High Impact
ID.AM-1: Physical devices and systems within the organization are inventoried	N: Not Achieved (0 to 15%)	1
ID.AM-2: Software platforms and applications within the organization are inventoried	N: Not Achieved (0 to 15%)	1
ID.AM-3: Organizational communication and data flows are mapped	N: Not Achieved (0 to 15%)	
ID.AM-4: External information systems are catalogued	N: Not Achieved (0 to 15%)	
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	N: Not Achieved (0 to 15%)	
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	N: Not Achieved (0 to 15%)	
ID.BE-1: The organization's role in the supply chain is identified and communicated	N: Not Achieved (0 to 15%)	
communicated	N: Not Achieved (0 to 15%)	
communicated	N: Not Achieved (0 to 15%)	
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	N: Not Achieved (0 to 15%)	
ID.BE-5: Resilience requirements to support delivery of critical services are established	N: Not Achieved (0 to 15%)	
ID.GV-1: Organizational information security policy is established	N: Not Achieved (0 to 15%)	
and external partners	N: Not Achieved (0 to 15%)	
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	N: Not Achieved (0 to 15%)	
ID.GV-4: Governance and risk management processes address cybersecurity risks	N: Not Achieved (0 to 15%)	

1
2
3
4
5

For each of the current profile items, evaluate the impact on your critical systems of not having this control in place. Consider this relative to the treat landscape

Click button to move data After paste is complete push Ctrl + Alt + L to refresh

Move Data

Threat	Risk Quotient
Advanced Persistent Threat Attack	Low
DDoS by External Party	Low
DDoS by Student	Low
Phishing Message Targeting Credentials	Low
(blank)	Low

Cyber Security Assessment Tool – Target Profile and Action Plan

- After completing the risk assessment, the data is then displayed on the target profile screen
- Users enter the desired state, taking into account the risk assessment data that was entered on the risk assessment screen.
- This view gives the user all the information needed to select a target profile that maps to the NIST objectives and takes risk into account.

Cyber Security Assessment Tool - Target Profile and Action Plan

Push Atl + F5 to refresh sub categories listing

Sub Category	Impact of not having control in place 1 = Low Impact 5 = High Impact	Current Profile Score	Desired State (Target)	Current Practices	Comments	Improvement Actions	Resources Required
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	(blank)	N: Not Achieved (0 to 15%)	F: Fully Achieved (>85%)				
DE.AE-2: Detected events are analyzed to understand attack targets and methods	(blank)	N: Not Achieved (0 to 15%)					
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	(blank)	N: Not Achieved (0 to 15%)	No Change				
DE.AE-4: Impact of events is determined	(blank)	N: Not Achieved (0 to 15%)					
DE.AE-5: Incident alert thresholds are established	(blank)	N: Not Achieved (0 to 15%)					
DE.CM-1: The network is monitored to detect potential cybersecurity events	(blank)	N: Not Achieved (0 to 15%)					
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	(blank)	N: Not Achieved (0 to 15%)					
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	(blank)	N: Not Achieved (0 to 15%)					
DE.CM-4: Malicious code is detected	(blank)	N: Not Achieved (0 to 15%)					
DE.CM-5: Unauthorized mobile code is detected	(blank)	N: Not Achieved (0 to 15%)					

N: Not Achieved (0 to 15%)
P: Partially Achieved (> 15 – 50%)
L: Largely Achieved (> 50 to 85%)
F: Fully Achieved (> 85%)

Cyber Security Assessment Tool – Gap Assessment

- The gap assessment page allows you to visualize easily the gaps between current sate and desired state
- This page also includes a calculation to help determine the priority of the gap as follows:
    - Gap score – Current state – target state
    - Gap score X impact = delta
    - Utopian score is 0 – no variance between current and target states, as well as no impact to not having the control in place
    - The higher delta the higher the priority for the subcategory (control)

Cyber Security Assessment Tool – Gap Assessment

Sub Category	Impact of not having control in place 1 = Low Impact 5 = High Impact	Current Status	Desired Status	Delta / 15 (Change * Impact) 0 = Minimal Change Low Impact 15 = High Change High Impact
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	5	N: Not Achieved (0 to 15%)	F: Fully Achieved (>85%)	15
DE.AE-2: Detected events are analyzed to understand attack targets and methods	5	N: Not Achieved (0 to 15%)	F: Fully Achieved (>85%)	15
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	5	N: Not Achieved (0 to 15%)	F: Fully Achieved (>85%)	15
DE.AE-4: Impact of events is determined	3	N: Not Achieved (0 to 15%)	L: Largely Achieved (>50 to 85%)	6
DE.AE-5: Incident alert thresholds are established	5	N: Not Achieved (0 to 15%)	L: Largely Achieved (>50 to 85%)	10
DE.CM-1: The network is monitored to detect potential cybersecurity events	5	N: Not Achieved (0 to 15%)	F: Fully Achieved (>85%)	15
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	5	N: Not Achieved (0 to 15%)	F: Fully Achieved (>85%)	15

Cyber Security Assessment Tool – Next Steps

- Supplemental scoring guides to better quantify each score – This is somewhat subjective in the interview stage.
- Improved UI
- Relational DBMS
    - Constructing this method in a database management system would allow for a tighter relationship between the controls and the threats.
    - Filters and PivotTables converted to SQL queries would make for easier (automatic) refresh of the data.

References and a Note on Sharing

NIST Framework

https://www.nist.gov/cyberframework

Some Work Based on ISACA

Implementing the NIST Cybersecurity Framework

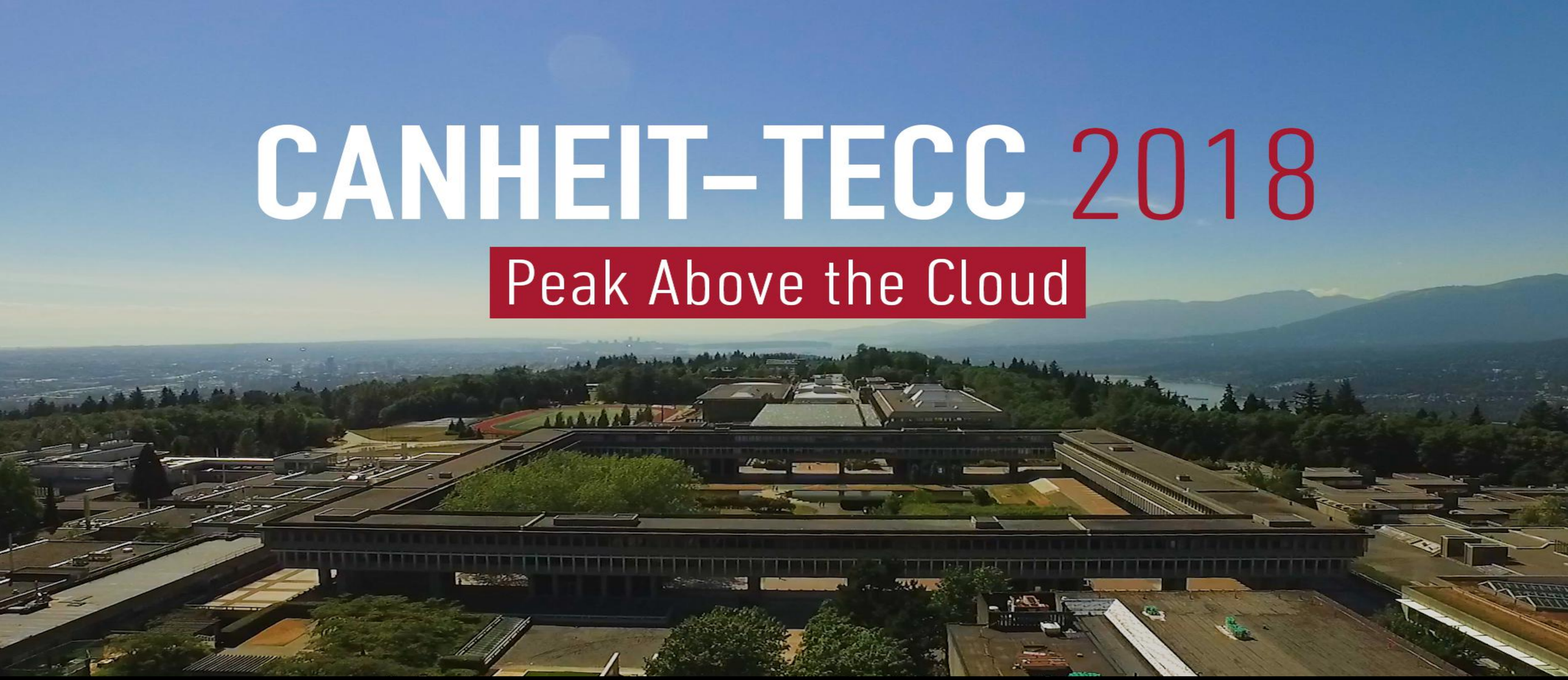
https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx

Cybersecurity: Based on the NIST Cybersecurity Framework

https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx

What can we Share?

Our presentation, our developed Excel template, and the VISIO templates for the Cybersecurity Maturity Radar



Questions