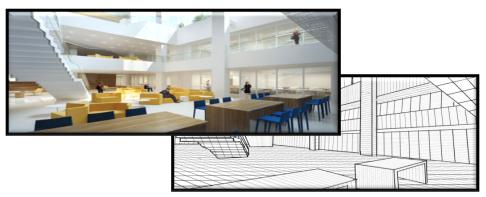
Improving The Operational Effectiveness of DHS'S Cyber Security Evaluation Tool (CSET)

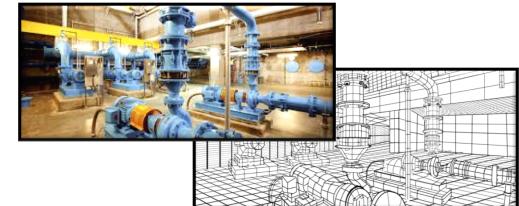
Researchers: Gilberto Castro Danny Seo Faculty Advisor: Henry J. Sienkiewicz

> GEORGETOWN UNIVERSITY



## Address the gap in ICS/SCADA/IoT cyber security assessments







## Background

- Georgetown University's School of Continuing Studies
  - Master of Professional Studies in Technology Management
  - 30 credit hours/on campus & online/full or part time
- Focused coursework and practical, hands-on experience.
- Specific Courses:
  - Summer 2018: MPTM 665-40: Perspectives in Addressing Cybersecurity & Critical Infrastructure: A National Challenge
  - Fall2018: MPTM 661-01: Information Assurance & Risk Assessment

#### Special thanks to:

- Mark Bristow
- Daryl Haegley
- Steven Chen
- Andrew Wonpat

https://scs.georgetown.edu/programs/77/master-ofprofessional-studies-in-technology-management/

- Research projects:
  - Summer 2018: Initial assessment use of CSET to identify vulnerabilities, and the initial application of the Microsoft DREAD model & Six Sigma QFD to evaluate and prioritize risk.
  - Fall 2018: Improvements to the assessment through extending the use of the DREAD model & QFD to CSET.

### Addressing the gap in ICS/SCADA/IoT cyber security assessments









### **Cyber Security Evaluation Tool**

#### What is CSET?

- Is a software program developed through conjunct effort between cybersecurity experts and NIST under the direction of the then ICS-CERT
- Provides a systematic and repeatable method of assessing cybersecurity posture
- Produces a comprehensive questionnaire based on Service Assurance Level
- Supports industry standards from NIST, NERC, TSA, DoD and other applicable
- Generates a range of reports from highlevel to detailed for a review

#### CSET's Key Benefits

- Helps with risk management and decision-making process
- Raises awareness and facilitates discussion
- Highlights vulnerabilities and provides recommendations
- Identifies areas of strength and best practices
- Provides a method to compare and monitor risk assessments over time
- Recognized as a common industry-wide tool for evaluating cyber systems



### Limitations of CSET

- CSET generates a set of reports focusing on the level of compliance
- Identifies areas needing attention based on its proprietary weighting
- <u>CSET indicates potential vulnerabilities, but stops</u> <u>there</u>
- <u>Useful, but.....</u>

### The results needed to become actionable

"Risk = Threat x Vulnerability"

Threats & Vulnerabilities must be identified <u>as a pair</u> in order to assess risk.



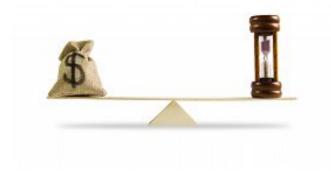
### **Adding Utility**

"Risk = Threat x Vulnerability"

#### Threats & Vulnerabilities must be identified <u>as a pair</u> in order to assess risk.

### Prioritization based upon

- Organizational drivers
- Accepted methodologies
- Standard frameworks
- Operational needs





### How can CSET be improved?

Repurpose existing, accepted industry standards

Prioritization based upon both qualitative and quantitative methodologies

**Ensuring that** 

"Risk = Threat x Vulnerability" Threats & vulnerabilities must be identified <u>as a pair</u> in order to assess risk.



**DREAD** for Qualitative



**QFD** for Quantitative



### **DREAD & QFD for CSET**

- DREAD: Qualitative Risk Analysis Method
  - Gives granular segmentation than conventional qualitative method (Risk = Impact x Likelihood)
  - D, R, E, A, D are not highly correlated
  - DREAD model is scalable from software bug classification to organizational cybersecurity risk assessment
  - Ranking gives a focus on worst vulnerabilities
- QFD applied to DREAD model
  - Transforms qualitative values (High, Medium, Low) into qualitative values that can be analyzed statistically.





#### **DREAD** for Qualitative



Sources: https://blogs.msdn.microsoft.com/david\_leblanc/2007/08/14/dreadful/; Knapp & Langill, 2015



### CSET, DREAD & QFD in Action (Notional)

Threat Agents	Exploit this vulnerability	Resulting in this threat	D	R	E	Α	D	Risk Score
Careless, Negligent & Indifferent Employees (CNI), and Intruder	No security awareness training	Falling prey to social engineering attacks (i.e., phishing, spear- phishing, whaling);	10	5	5	10	5	7
	Lack of training for security policies, procedures, and processes including mandatory security programs	Violation of regulatory requirements (i.e., NERC, FERC, FISMA, etc.)	10	10	10	10	10	10
CNI, Contractor	Missing or poor definition of incident response plan or procedure including roles and responsibilities, communication channel; No regular exercise and maintenance of incident response plan	Possible to miss the golden time to respond to security incidents, resulting in greater damage on finance, reputation, and even human casualties	10	10	5	10	10	9
CNI, Intruder	No security protection (i.e., encryption, additional credentialing) commensurate with the sensitivity level of data stored in mobile devices	Increasing the attack surface as mobile devices with remote access capability are an extension to the corporate network (and ICS network only if HMI application is installed)	5	5	1	5	10	5.2



### **Research Conclusions**

- DREAD & QFD enhances risk analysis in CSET.
- DREAD model involves judgment of assessor(s) when evaluating each threat and vulnerability & ranking risk.
- Given subjectivity, it is important to exercise consistency throughout the risk assessment and future assessments.

### **Potential Next Steps**

- Enhance and automate the CSET tool to include the DREAD & QFD
- Continue development on standard , specifically an ICS AT&TK framework
- Include attack tree analysis and SHODAN results

### **Editorial Observation**

• This type of actionable research is a great example of potential partnerships between academia, government, and commercial organizations.

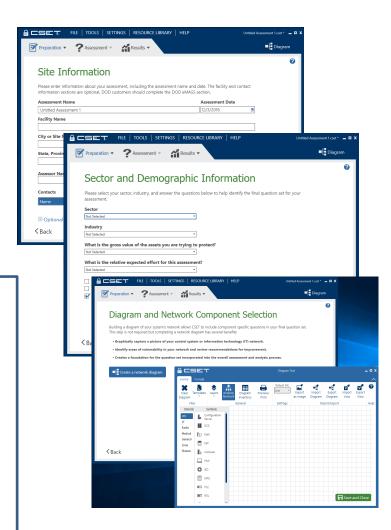






### A Bit Of A Primer: "How does CSET work?"

- Step 1: Provide Site Information
- Step 2: Define the Sector and the Demographics
- Step 3: Diagram & Network Component Selection
- Step 4: Mode selection
- Step 5: Service Assurance Level
   Definition
- Step 6: Answer the generated questions





Source: CSET Version 8.1

#### Step 4 - Mode selection: Basic or Advanced

#### **Basic Mode**

- Uses the provided demographic information
- Selects appropriate default questions
- Does not reference cybersecurity standards.
- Appropriate for

- Organizations that are not regulated by a particular industry

- Are in the developmental stage of a cybersecurity program.

#### **Advanced Mode**

- Questions-based approach uses simple questions.
- Requirements-based approach uses the exact wording from a standard and is best suited for those industries regulated by a specific standard.
- Cybersecurity framework-based approach allows the assessor to define a custom profile based on the Cybersecurity Framework.

	Assessment 1.cset * 🗕 🗖 🗙
Preparation 👻 ? Assessment 👻 🏭 Results 👻	■{ Diagram
Mode Selection	0
CSET contains a vast amount of cybersecurity knowledge. Please indicate whether you want an auto-generated quest set, or if you would prefer to build your own question set by selecting from cybersecurity standards.	ion
O Basic - Generate a basic assessment using the provided demographic information	
Advanced - Let me choose which cybersecurity standard(s) the assessment will be based on:	
Enfore selecting which operacounty standards your assessment is based on please choose one of the following options.  O Questions based Approach The question-based approach was imple questions and allows for partial credit.  Requirements based Approach The question-based approach uses the exact wording of the standard and is best for those industries that are required by a people standard approach uses allowed Approach The question of the question of the standard and is best for those industries that are required by a people standard approach uses allowed Approach The question of the question of the standard and is best for those industries that are required by a specific standard.  @ Question: The question of the question of the standard and is best for those industries that are required by a specific standard.  @ Question: The question of the question of the standard and is best for those industries that are required by a specific standard.  @ Question: The question of the question of the standard and is best for those industries that are required by a specific standard.  @ Question: The question of the question of the standard and is best for those industries that are required by a specific standard.  @ Question: The question of the questi	lated
< Back	Continue >>



### Step 5 – Security Assurance Level (SAL) Definition

- Level selection
- Low SAL typically 30 to 350 questions
- High SAL typically 350 to 1,000 questions
- Standards selection
- Framework based approach
- Baseline framework is automatically populated
- Implementation tiers
- Properties
  - Risk management processes
  - Integrated risk management program
  - External participation
- Each property has fours tiers representing a level of maturity

	ent 1.cset * 🕳 🗖 🗙				
Preparation • ? Assessment • Aff Results •	Diagram				
Cybersecurity Framework	0				
Select the cybersecurity framework profile you want to use for your assessment. The baseline cybersecurity framework profile prebaded with CSFT that you can cogy to get started when creating your own custom profiles. You can also create a new cu profile or update and export existing profiles.					
Profile Implementation Tiers	_				
Your Overall Tier Level is: Tier 1: Partial					
Risk Management Process Integrated Risk Management Program External Participation					
Tier 1 © Opperational opheracolity nik management practices are not formalised, and nik in managed in an ad hoc and isometimes reactive manover Prioritization of opheraconity achivities may not be directly informed by organizational risk objectives, the threat environment, or business/imasion requirements.					
Tier 2 O Rick management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities of activity informed by organizational nick objectives, the threat environment, or business/traision requirements.					
Tier 3 experiment practices are formely approved and expensed as poly. Operational operational processing practices are regularly optimate based on the application of risk management processes to changes in business/mission requirements and a changing these and technology landcape.					
Tier 4 O The ognitation adapts its givenesserity practices based on testors learned and predictive indicators derived from previous and current optenessionly schules. Through a process of continuous improvement incorporating advanced optenessing technologies and practices, the organization schuley adapts to changing optenessionly landscape and responds to evolving and sophistcated threads in a timely mannee.					
<back conti<="" td=""><td>inue &gt;&gt;</td></back>	inue >>				

CSET determines the overall tier level and the equivalent SAL for the assessment, which are commensurate with the total number of questions.



### Step 6 - Answer the generated questions

Every question provides detailed supplemental information that provides guidance to the assessor in the subject being questioned.

	SOURCE LIBRARY   HELP Untitled Assessment 1.cset * X
Preparation	sults 🔻 📕 Diagram
All + Cybersecurity Framework + Identify + Asset Mar	nagement Search P Filter * 😮
Asset Management	
1 Physical devices and systems within the organizatio	in are inventoried
O Yes	Supplemental Information
O No	Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizatione ensure that the resulting inventories include system-specific information required
O Not Applicable	for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system
O Alternative Response	Read more
View details and resources or add comments	🗆 Mark For Review 🛛 💬 📄 💡
2 Software platforms and applications within the orga	anization are inventoried
O Yes	Supplemental Information
O No	Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations,
O Not Applicable	organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system
O Alternative Response	Read more
View details and resources or add comments	🗆 Mark For Review 🔛 皆 🖓
3 Organizational communication and data flows are r	mapped
O Yes	Supplemental Information
O No	Supplemental Guidance from NIST 800-53 Rev 4, AC-4
O Not Applicable	Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that
O Alternative Response	Read more
View details and resources or add comments	🗆 Mark For Review 🔛 🖹 💡 🖕
Mode: Cybersecurity Framework Profile: Baseline Cybersecurity Framework	Questions Complete 0 / 98



### **Generate CSET Reports**

	Untitled Assessment 1.cset * 🕳 🗖 🗙
Preparation • ? Assessment • 🎢 Results •	<b>■{</b> ∎Diagram
Report Builder	0
Create your final reports in PDF or DOCX format. You can add descriptions, comments and an executive s reports. You can also specify comments, descriptive text and an executive summary to your reports as we specific sections for the Detail report.	
Select the reports you want to build  Executive Summary Security Plan Detail Report Sectors *	
Select the file type  PDF DOCX Category Create Report(6)	
Status	
N DOLK	
PDF	

- Executive Summary
- Site Summary
- Security Plan
- Other detailed reports
- Component Gap Analysis

#### Again, useful but.....

#### The results needed to be prioritized and actionable



Source: CSET Version 8.1

### Microsoft DREAD Model

- Bill Gates' "Trustworthy Computing" memo (2002) as available, reliable, and secure as electricity, water services and telephony
- "Writing Secure Code" by Michael Howard & David LeBlanc introduced STRIDE and DREAD as part of threat modeling
- DREAD Model originally developed to classify software bugs
- DREAD <u>D</u>amage potential, <u>R</u>eproducibility, <u>E</u>xploitability, <u>A</u>ffected users, and <u>D</u>iscoverability

Source: https://www.wired.com/2002/01/bill-gates-trustworthy-computing



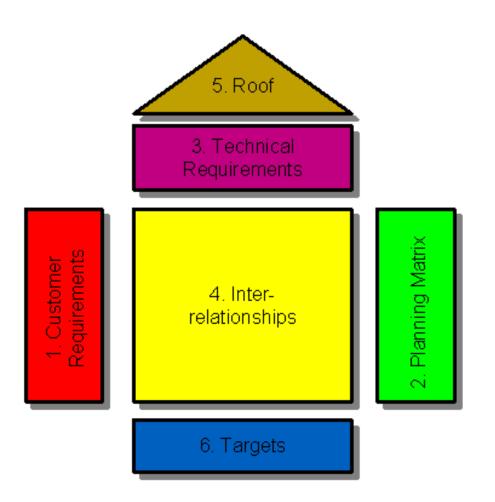
### Microsoft DREAD Model (Cont.)

	Rating	High	Medium	Low	Indirectly Measures
D	Damage potential	Attacker can subvert the security; get full trust authorization; run as administrator; upload content	Leaking sensitive information	Leaking trivial information	Consequences
R	Reproducibility	Attack can be reproduced every time; does not require a timing window; no authentication required	Attack can be reproduced, but only with a timing window and a particular situation; authorization required	Attack is very difficult to reproduce, even with knowledge of the security vulnerability; requires administrative rights	Likelihood
E	Exploitability	Novice programmer could make the attack in a short time; simple toolset	Skilled programmer could make the attack, then repeat the steps; exploit and/or tools publicly available	Attack requires an extremely skilled person and in-depth knowledge every time to exploit; custom exploit/tools	Likelihood
Α	Affected Users	All users; default configuration; key assets	Some users; non-default configuration	Very small percentage of users; obscure feature; affects anonymous users	Consequences
D	Discoverability	Published information explains the attack; vulnerability is found in the most commonly used features; very noticeable	Vulnerability is in a seldom- used part of the product; only a few users should come across it; would take some thinking to see malicious use	Bug is obscure; unlikely that users will work out damage potential; requires source code; administrative access	Likelihood



### **Quality Function Deployment**

- Product design method developed in Japan in 1966
- "House of Quality"
- Transforms <u>qualitative</u> user demands into <u>quantitative</u> parameters related to organizational capabilities





### QFD Likelihood & Impact Definitions

Likelihood	Definition
Low	0–33% chance that the event will occur in a 12-month period
Medium	34–66% chance that the event will occur in a 12-month period
High	67–100% chance that the event will occur in a 12-month period

Impact	End-user Impact	Economic Damage	Damage to Business Operations	Potential for Litigation
Low	No harm to end- user	<us \$10k<="" th=""><th>Unavailable for less than an hour</th><th>Low</th></us>	Unavailable for less than an hour	Low
Medium	End-user data damaged but no direct physical effects	US \$10K < damage < US \$100K	Unavailable between 1 and 4 hours	Medium
High	End-user data damaged causing adverse effects on end-user	Damage > US \$100K	Unavailable over 4 hours	High



Source: Touhill & Touhill, 2014

# Thank you



GEORGETOWN UNIVERSITY