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

Researchers:

Gilberto Castro

Danny Seo

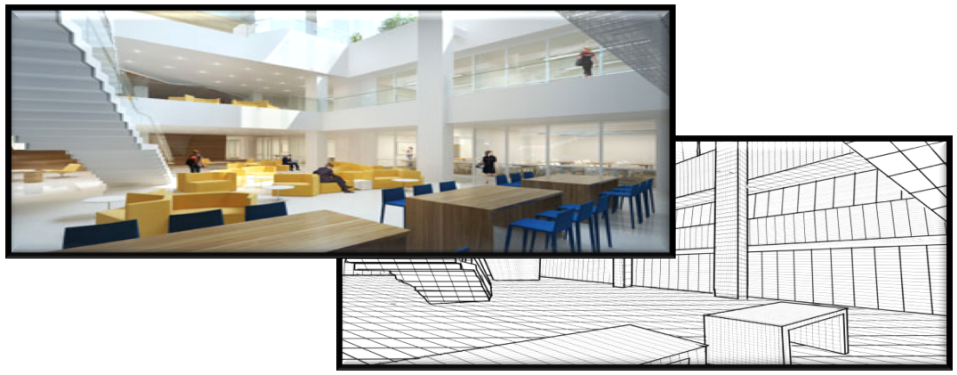
Faculty Advisor:

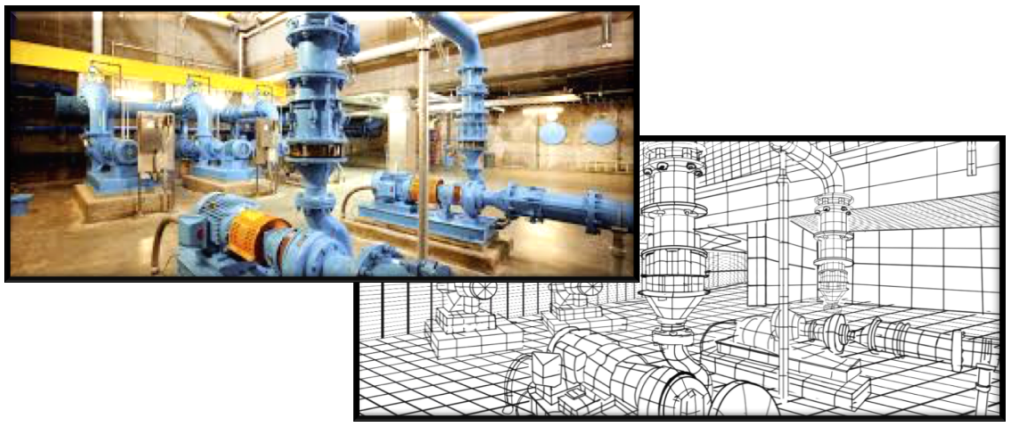
Henry J. Sienkiewicz

GEORGETOWN UNIVERSITY

So why?

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





Background

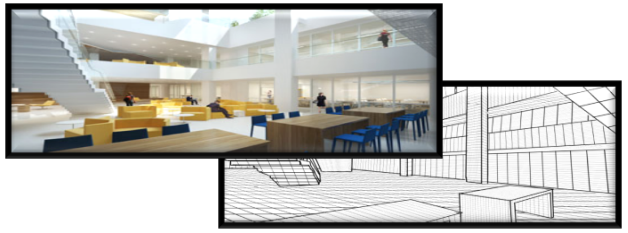
- Georgetown University's School of Continuing Studies
  - Master of Professional Studies in Technology Management
  - 30 credit hours/on campus & on-line/full or part time
- Focused coursework and practical, hands-on experience.
- Specific Courses:
  - Summer 2018: MPTM 665-40: Perspectives in Addressing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

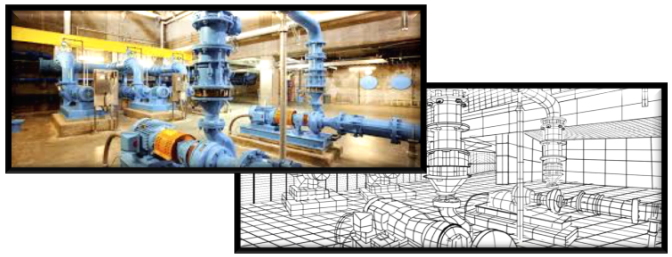
Special thanks to:

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

- 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





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

GEORGETOWN UNIVERSITY

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 high-level 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

Source: https://cset.inl.gov/SitePages/Home.aspx

Limitations of CSET

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

The results needed to become actionable

"Risk = Threat x Vulnerability"

Threats & Vulnerabilities must be identified as a pair in order to assess risk.

Adding Utility

"Risk = Threat x Vulnerability"

Threats & Vulnerabilities must be identified as a pair 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 as a pair in order to assess risk.

DREAD for Qualitative

6σ

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

DREAD for Qualitative

- QFD applied to DREAD model
  - Transforms qualitative values (High, Medium, Low) into qualitative values that can be analyzed statistically.

6σ

QFD for Quantitative

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	A	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
CNI, Contractor	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
	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

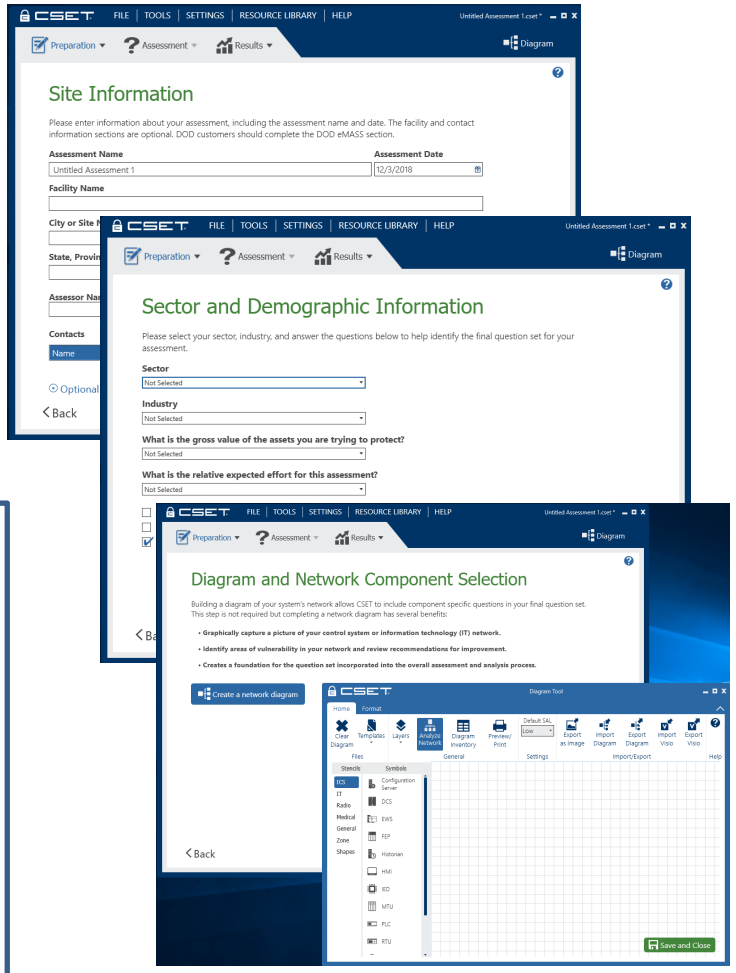
Editorial Observation

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

BACKUPS

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



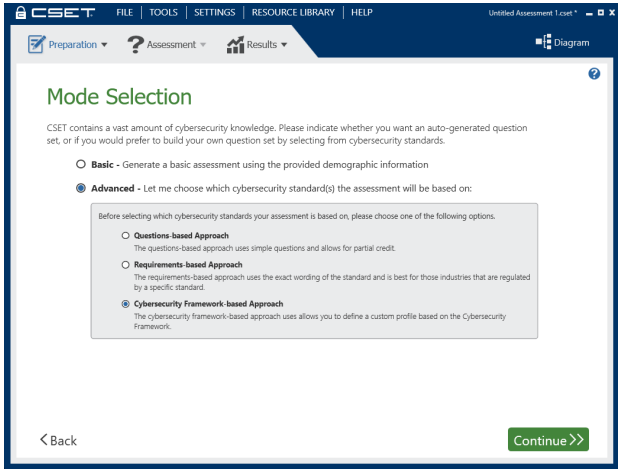
Source: CSET Version 8.1

GEORGETOWN UNIVERSITY

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.



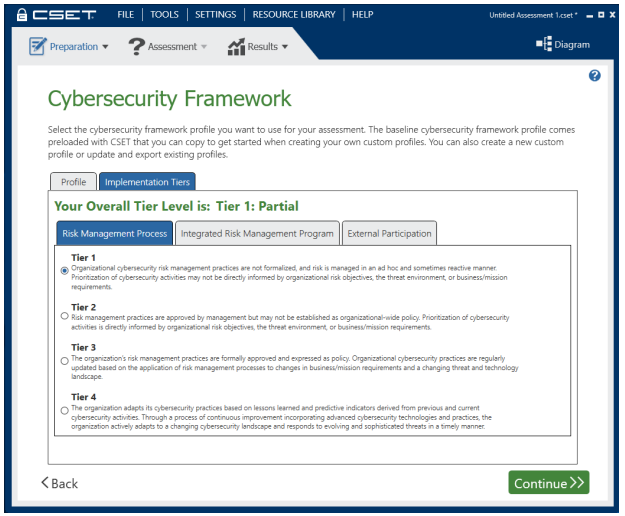
Advanced Mode

- 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.

Source: CSET Version 8.1

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

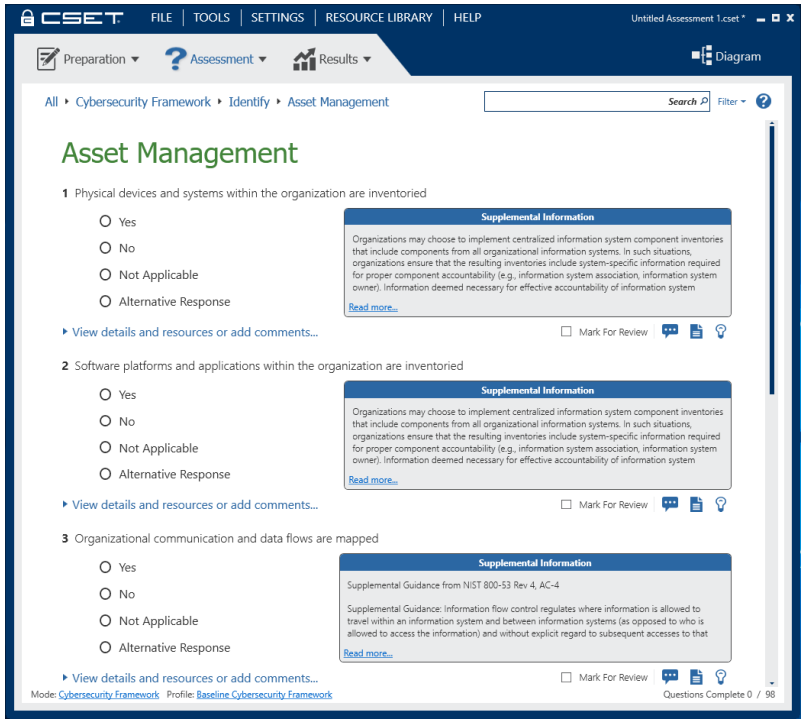


CSET determines the overall tier level and the equivalent SAL for the assessment, which are commensurate with the total number of questions.

Source: CSET Version 8.1

Step 6 - Answer the generated questions

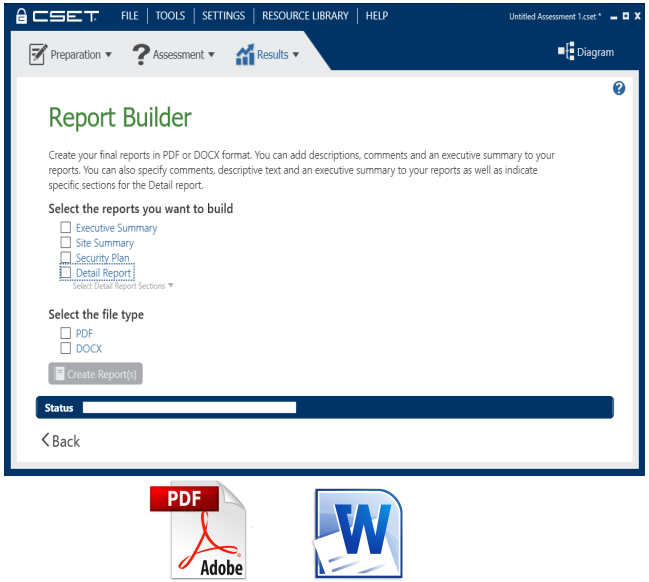
Every question provides detailed supplemental information that provides guidance to the assessor in the subject being questioned.



Source: CSET Version 8.1

GEORGETOWN UNIVERSITY

Generate CSET Reports



- 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 - **D**amage potential, **R**eproducibility, **E**xploitability, **A**ffected users, and **D**iscoverability

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

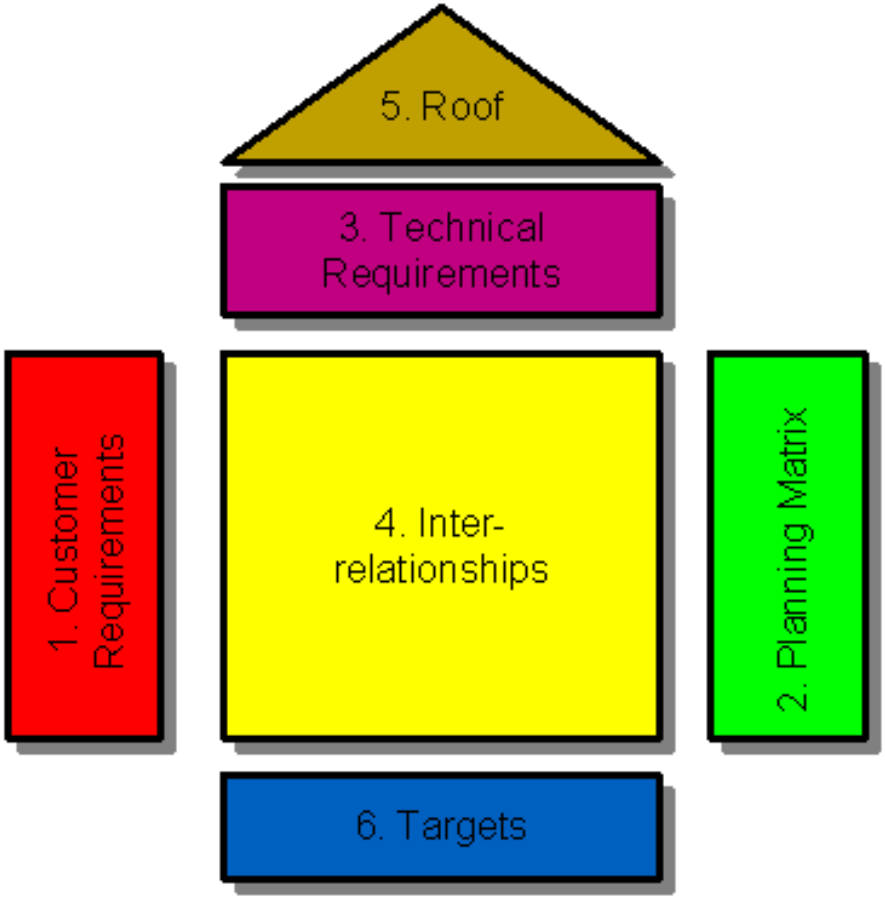
Microsoft DREAD Model (Cont.)

	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
A	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

Sources: Howard & LeBlanc, 2002; Knapp & Langill, 2015

Quality Function Deployment

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



Sources: https://www.sixsigmadaily.com/six-sigma-and-quality-function-deployment/
https://sixsigma.com.my/training/product/quality-function-deployment/

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	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