

Integrated Virtual Learning Environment for Cybersecurity (IVLE4C)

Being Developed @ UNCW by
Jeff Greer, Dr. Geoff Stoker, Dr. Ulku Clark
AMCIS TREO Brief
August 2022



OBSERVED CLASSROOM PROBLEM

Cybersecurity students do not understand the structure, operations and control of a modern digital enterprise.

Currently this knowledge is learned experientially on the job post graduation.



WHY IS THIS A BIG DEAL?

It is impossible to defend a modern digital enterprise if it cannot be visualized and described.

There are material benefits to be gained if this problem can be solved!



POTENTIAL SOLUTION BENEFITS

Improve cybersecurity pedagogy - teach enterprise cybersecurity first to establish a better context for learning single topic cybersecurity classes.

Accelerate student cybersecurity skill development so they are better prepared to contribute on day one of their employment.



Big Question - How Can the Cybersecurity Classroom Experience Be Improved ???



Old School -
Passive Learning



New (Exciting) School -
Active Learning

Hint – Look at What Others Are Doing IE Digital Cadaver Use In Medical Training



What is the Analog then for Teaching “Enterprise” Cybersecurity ???



Use Models In the Classroom In Lieu of, or Supplemental to, Experiential Learning

Create An Integrated Virtual Learning Environment for Cybersecurity (IVLE4C)

Digital Business Theory



A Parametric Data
Driven Web Application
For Student Use

*Model-Based Systems
Engineering Theory*

Cybersecurity Theory

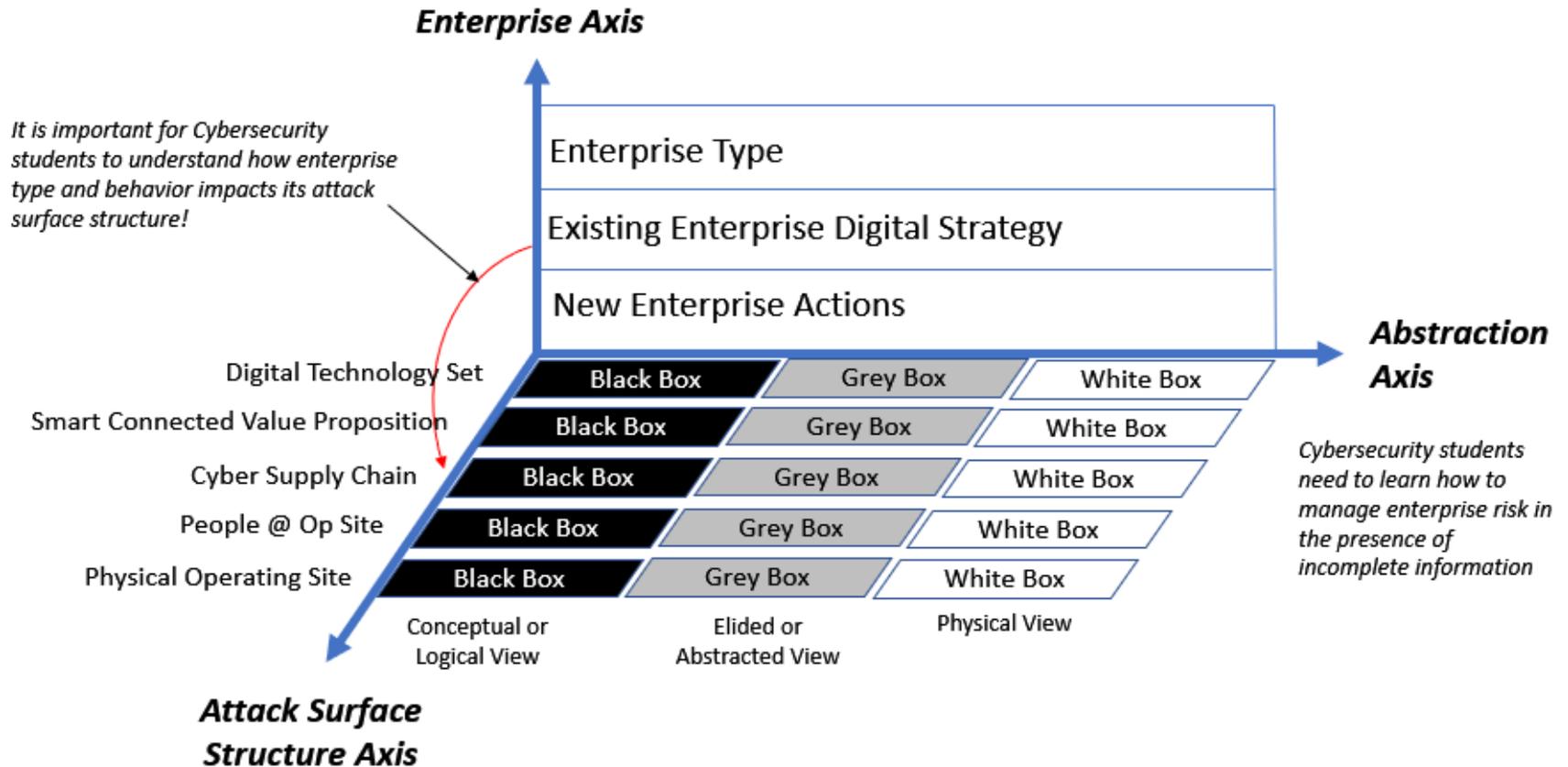
Teach Enterprise Cybersecurity By Design – Build Upon the Seminal
Work by Nancy Mead Which Was IT Project Centric



IVLE4C Risk Treatment Work Process

Four Step Work Process	Work Process Inputs From Exemplar or Targeted Research Findings	Work Process Outputs
Model	Research Findings About The Enterprise Being Defended	Descriptive Enterprise System Model (DESM)
Analyze	<ul style="list-style-type: none"> - Assets of Value - Named Threats - Untreated Vulnerabilities - Named Risks Ranked By Importance - Compliance Requirements - Security Requirements - Enterprise Risk Appetite 	Risk Register
Design	Risk Register	Risk Treatment Plan Based On ISO 31000 Options and Selected Security Controls
Implement	Risk Treatment Plan	Plan of Action With Milestones (POAM)

Proposed Descriptive Enterprise System Model (DESM) – an Artifact for Classroom Use

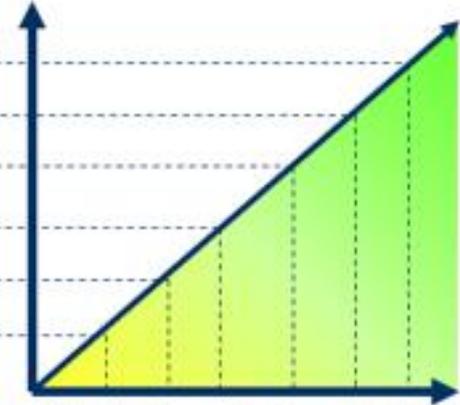


Create A Two Dimension DESM Library For Teacher and Student Classroom Use



IE Transportation Sector
Port of Los Angeles

Workplace Professionals
Cybersecurity Researchers
Graduate Students
University Students
Community College Students
K-12 Students



Beginning Student -
Conceptual or
Heavily Abstracted
Cybersecurity
Education Content

Advanced Student -
Slightly Abstracted
or Near Real
Cybersecurity
Education Content

DESMs Based On
Enterprise Type



DESMs To Meet Student
Learning Needs



A Look at the Near Future

[Home](#) | [UNCW](#) | [CCDE](#) | [Career Info](#) | [Contact Us](#) | [Login](#) | [Logout](#)



Website In Development

Home	Welcome!
Use Case	IVLE4C Use Case
Work Process	IVLE4C is a virtual learning environment for training students to think and act like a Chief Information Security Officer (CISO) who has been tasked to protect a modern digital enterprise against cyber risks.
Model (DESM)	
Analyze (AoV)	Background on Enterprise Cybersecurity
Analyze (Threats)	Within the cybersecurity theory domain, enterprise cybersecurity deserves special consideration because a modern digital enterprise is a large-scale complex system of systems. Students need to develop specialized skills for managing enterprise cybersecurity.
Analyze (Vulnerabilities)	
Analyze (Risk)	Targeted Student Educational Outcomes:
Analyze (LRC)	Students will learn a four-step work process for creating an enterprise risk treatment plan.
Design (RTP)	The four steps are model, analyze, design and implement.
Implement (RTP)	In the model step students will learn how to develop and use a descriptive enterprise system model (DESM). The DESM will teach students how enterprise type and behavior impact its attack surface structure.
Dashboard	In the analyze step students will learn how to identify assets of value, develop a profile of threats facing the enterprise, identify inherent or untreated vulnerabilities that a threat actor can exploit, create a risk register, and assess and order risks using a heat map.
Site Maintenance	In the design step students will learn how to treat risk and convert the enterprise attack surface into a trust boundary at a level sufficient for achievement of security objectives. Named risks will be treated with an ISO 31000 option and a security control when applicable and appropriate. A review and treatment of risks results in a risk treatment plan.
	In the implement step students will learn how to create a plan of action and milestones for implementing the risk treatment plan.
	Page last updated: Mon 18 July 2022

Copyright © 2022 University North Carolina Wilmington



UNCW® Center for Cyber Defense Education

ONE FINAL POINT FOR CONSIDERATION

*My Dad taught me to use the best tool
for the task at hand.*

*A cyber-range is network centric and
IVLE4C is enterprise centric!*



IVLE4C Questions & Feedback

Jeff Greer

greerj@uncw.edu

401-714-1141

