
CBC
Columbia
Basin College
We All Soar Together

Eric Robinson

Cyber Security
Assistant Professor, Cyber Security

Email: erobinson@columbiabasin.edu
Office hours: Zoom online

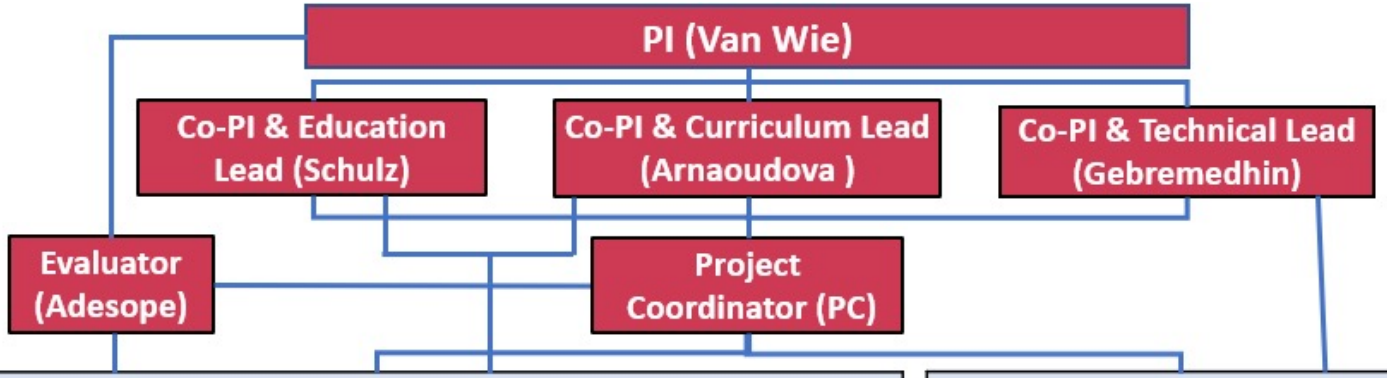
Matt Boehnke

Cyber Security
Assistant Professor, Cyber Security

Email: mboehnke@columbiabasin.edu
Office hours: Zoom online

CBC
Columbia Basin College

CySER – Organization



Education Thrust Coordinators: WSU, MSU, UI, CBC, CWU		
CySER Basics Certification (Crossler, Jillepalli)	CySER & CAE-CO Certification (Jillepalli)	Internships & ROTC (Schulz)
Curriculum (Arnaoudova, Crossler, Bo ke, Soule, Izurieta)		
Faculty Develop. & Assess. (Hundhausen, Adesope, Van Wie)		
ROTC Interns (Lt. Cols. Balazs, Ratterman, M rris, Maj. Hyde, PC) Civilian Interns (Schulz, Izurieta, Soule, Bo ke, PC)		
Seminars (All CySER Faculty, PhD Trainees, PC)		
Workshops (Van Wie, Balazs, Ratterman, Morris, Gebremedh n, PC)		
High Sch./New Std. /Comp. (ROTC Instrs., Gebremedhin, Bo ke, PC)		

Research Thrust Leads: WSU, MSU, UI, CBC
Cyber Education (Hundhausen)
Networks & Information Security (Holder, R son)
Cyber-Physical Systems (Pande)
Machine Learning & AI (Doppa, Soule)
Software Security & Quality Assurance (Cai, Izurieta)

CBC CySER

- Who are the CyberHawks
- Competition
- Community Outreach/ Internships
- Research- Prof Robinson
- Questions?

Cyber Security Program

- Started 2014
- Degree Pathways
  - Short Term or 1 year Certifications
  - 2 year AAS;
  - BAS in Cyber Security
  - *Added BAS in Information Technology (2020)
  - Working on: data analytics/ cloud services
- Graduates: 4 - 2015, 28 - 2017 (600% increase)
- Over 85% job placement; average salary: $65,000

CERTIFIED AS A NATIONAL CENTER OF ACADEMIC EXCELLENCE (CAE2Y)

Designation is certified by the National Security Agency (NSA) and the U.S. Department of Homeland Security due to the college's proof of commitment to excellence in the field of Information Assurance and Cyber Defense Education.

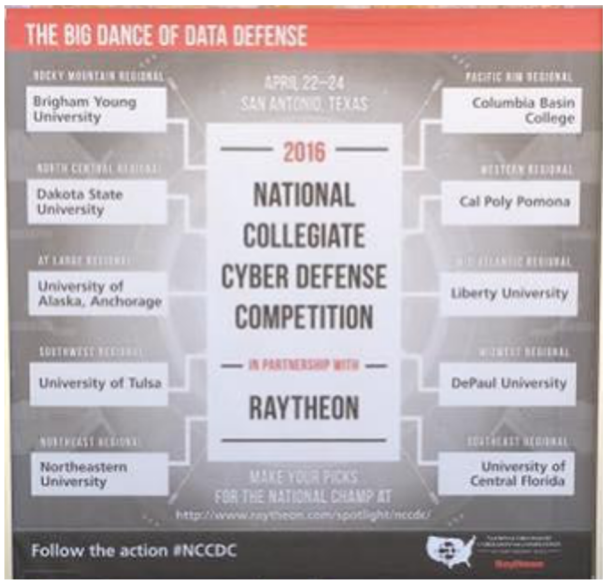
Columbia Basin College

Cyber Security Division

CYBERHAWKS

"Vigilance, quick thinking pays off for CBC cybersecurity students"

TCH, April 15, 2016



Competition

- Pre Event
- Before start – Last minute prep
- Hardening Critical Services
- Web App Exploitation
- Compromising the Network
- Social Engineering
- Physical Attacks
- Evading AV and Network Detection
- SoftSkills
- Post Event Analysis

"Don't Forget the Basic 13"

Dwayne Williams, National CCDC Director, CCDC post

CBC Outreach

- **Internships (PAID)**
  - Pacific Northwest National Labs (PNNL)
  - Amazon
  - Department of Energy/Ecology
    - Office of River Protection
    - Hanford Laboratory Management & Integration
    - Bechtel National, Inc (BNI)
    - Washington River Protection Solutions LLC (WRPS)
    - DOE Richland Operations Office
    - Hanford Mission Essential Services
    - HPM Corporation (HPMC)
    - CH2M Remediation Company
    - Mission Support Alliance (MSA)
  - State Agencies
    - Department of Commerce/Port of Benton
    - Energy Northwest (Nuclear/Solar/Wind)
  - Regional
    - City of Richland- Solar/ Battery Storage
    - Darklight
    - Marcraft
    - Port of Kennewick (Ransomware 2020)

Cyber Security Program

mappings + highlights

course	Certified Information Systems Security Professional (CISSP) domain mapping	certification mapping	highlights	
			security operations	security research
CSIA 320: Ethical Hacking	• Asset Security • Software Development Security	Certified Ethical Hacker (CEH)	Analyze ARP cache poisoning attack.	**Use algorithmic approach to predict malware infection rates.**
CSIA 330: Wireless Security	• Communication and Network Security	Certified Wireless Security Professional (CWSP)	Assess and strengthen wireless security assets.	Remediate smart meter firmware vulnerability.
CSIA 420: Cyber Crime and Terrorism	• Security and Risk Management • Security Operations		Quantify cybersecurity risk using Monte Carlo methods.	**Optimize control selection to minimize cybersecurity risk.**
CSIA 440: Cyber Testing and Penetration	• Security Assessment and Testing		Complete full penetration test on physical production network.	Predict phishing email success based on keyword analysis.
CSIA 450: Cyber Security Capstone	• Security Architecture and Engineering • Identity and Access Management		Assess mobile device security models and vulnerabilities.	Predict social engineering success based on human risk indices.

Research predict malware infection rates

Much research has been done to determine the feasibility of predicting malware infections from system and user attributes. Datasets can be gathered that contain various properties of each machine and the actual infection status of each machine, generated by an endpoint anti-malware solution.

Endpoint	Department	Risk Total	Data Classification	Function	Operating System	Network Security Zone	Firewall Level	Patch Level	Malware?
m83	Legal	Critical	Confidential	Database Server	Linux	Management	None	Scheduled	Yes
m121	Sales	High	Internal	Database Server	Microsoft Windows	Internet DMZ	Network-Based	Ad-Hoc	No
m122	HR	Low	Internal	Database Server	Legacy	Intranet Zone	None	Scheduled	No
...	...	...	...	...	...	...	...	...	....

1. Students are given 10,000 records of known malware infections and their attributes.
2. Students are given 1,000 records of known malware infections with separate results for testing.
3. Students develop their own algorithms and approaches for solving this problem. Some write machine learning code and some use Excel pivot tables.
4. Students apply their solution to a 10-record problem set.

Research optimize control selection

Rebound Security has decided to implement a set of risk mitigation controls to strengthen its security posture against future penetration tests and possible attacks.

Control_ID	Control_Description	Labor_Cost ($)	System_Cost ($)	Risk_Reduction ($)
C1	Implement application whitelisting.	150000	50000	100000
C2	Patch 3rd party applications.	100000	100000	100000
C3	Harden user applications.	75000	125000	100000
C4	Educate users on how to avoid phishing emails.	100000	400000	1000000
C5	Deploy advanced anti-malware software.	250000	250000	1000000
C6	Patch operating systems.	500000	300000	1300000
C7	Implement multi-factor authentication.	200000	100000	700000

1. How many ways could the controls be implemented? For example, you could implement C1, but not C2-C7. Or you could implement C1 and C2, but not C3-C7. Or you could implement C7, but not C1 - C6.

2. If there is a budget maximum of $1,000,000, what is the subset of controls that Rebound Security should implement to maximize the COUNT of controls implemented?

3. If there is a budget maximum of $1,000,000, what is the subset of controls that Rebound Security should implement to maximize the VALUE of controls implemented?

4. If there is a budget maximum of $1,000,000, what is the subset of controls that Rebound Security should implement to maximize the VALUE DENSITY of controls implemented?

5. If there is a budget maximum of $1,000,000, what is the optimal solution of controls for Rebound Security to implement?

Students then apply their learnings to a more complicated set of 37 possible controls based on the Australian Cyber Security Centre (ACSC)'s prioritized mitigation strategies.

Cyber Security Program

planned CySER enhancements

course	timeline	area	
		theory	practice
CSIA 320: Ethical Hacking	Planned for Spring 2022.	Increase foundational content in cloud security, web application security, and application security.	• Develop projects for each of these three areas.
CSIA 330: Wireless Security	Complete for Winter 2022.	Increase foundational knowledge in the electromagnetic spectrum.	• Review and summarize a relevant cybersecurity research paper in this area.
CSIA 440: Cyber Testing and Penetration	Planned for Fall 2023.	Increase foundational content in reverse engineering and malware pedigree.	• Enhance malware assessment to include pedigree. • Develop new assessment for reverse engineering.
CSIA 450: Cyber Security Capstone	Planned for Fall 2023.	Increase foundational content in data science and data science theory and ensure mathematical foundations of cryptography.	• Provide data science and data science theory topics for capstone projects. • Enhance cryptography assessment to include more rigorous mathematical foundations.

Thank you

CBC Columbia Basin College


CBC
Columbia
Basin College
We All Soar Together