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
CySER – Organization

**PI (Van Wie)**
- Co-PI & Education Lead (Schulz)
- Co-PI & Curriculum Lead (Arnaoudova)
- Co-PI & Technical Lead (Gebremedhin)

**Evaluator (Adesope)**

**Project Coordinator (PC)**

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

**Research Thrust Leads:** **WSU, MSU, UI, CBC**
- Cyber Education (Hundhausen)
- Networks & Information Security (Holder, 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
“Vigilance, quick thinking pays off for CBC cybersecurity students”
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

<table>
<thead>
<tr>
<th>course</th>
<th>Certified Information Systems Security Professional (CISSP) domain mapping</th>
<th>certification mapping</th>
<th>highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSIA 320: Ethical Hacking</td>
<td>• Asset Security</td>
<td>Certified Ethical Hacker (CEH)</td>
<td>Use algorithmic approach to predict malware infection rates.</td>
</tr>
<tr>
<td></td>
<td>• Software Development Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSIA 420: Cyber Crime and Terrorism</td>
<td>• Security and Risk Management</td>
<td></td>
<td>Optimize control selection to minimize cybersecurity risk.</td>
</tr>
<tr>
<td></td>
<td>• Security Operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSIA 440: Cyber Testing and Penetration</td>
<td>• Security Assessment and Testing</td>
<td></td>
<td>Predict phishing email success based on keyword analysis.</td>
</tr>
<tr>
<td></td>
<td>• Identity and Access Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

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

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

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

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

<table>
<thead>
<tr>
<th>course</th>
<th>timeline</th>
<th>area</th>
<th>practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSIA 320: Ethical Hacking</td>
<td>Planned for Spring 2022.</td>
<td>Increase foundational content in <strong>cloud security</strong>, <strong>web application security</strong>, and <strong>application security</strong>.</td>
<td>• Develop projects for each of these three areas.</td>
</tr>
<tr>
<td>CSIA 330: Wireless Security</td>
<td>Complete for Winter 2022.</td>
<td>Increase foundational knowledge in the <strong>electromagnetic spectrum</strong>.</td>
<td>• Review and summarize a relevant cybersecurity research paper in this area.</td>
</tr>
<tr>
<td>CSIA 440: Cyber Testing and Penetration</td>
<td>Planned for Fall 2023.</td>
<td>Increase foundational content in <strong>reverse engineering</strong> and <strong>malware pedigree</strong>.</td>
<td>• Enhance malware assessment to include pedigree.</td>
</tr>
</tbody>
</table>
| 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