

How to Develop a Cybersecurity Clinic

The Consortium of Cybersecurity Clinics
UT Austin Applied Cybersecurity Community Clinic

Francesca Lockhart, UT Austin Clinic Director



Agenda

- Intro to Clinics
- Clinic Foundation
- Clinic Curriculum
- Clinic Funding and Kickoff
- Student & Client Recruitment
- Clinic Metrics: Learning & Impact
- Summary and Q&A



**The Consortium of
Cybersecurity Clinics**

Cyber Clinics: Why Build One?

1

Provide **free services** to low-resource community organizations

2

Train a **multidisciplinary group of students** for the **cybersecurity workforce**

3

Promote **volunteerism** and provide **community service to locality**

Meet the UT Austin Cyber Clinic @



- Founded in 2023

Fall 2023: 19 students

- Cybersecurity Foundations
- Journey through the NIST CSF Core Functions

Spring 2024: 5 clients

- Cybersecurity Practicum
- 2 Small Businesses
- 1 Faith-based Nonprofit
- 2 City Governments
- 18 New Students

Fall 2024: 6 clients

- 32 New Students

Meet the Consortium of Cybersecurity Clinics



U.S. Consortium member clinic locations as of June 2024

- Founded in 2021
- 25+ active clinics and allies
- Join us!
cybersecurityclinics.org

Consortium Overview



Sharing and standardizing teaching materials among members



Supporting funding for the creation of new clinics



Advocating for the clinic model

- International educators **meet monthly** to share ideas, challenges, resources
- **Fundraising** and **Learning & Impact** Subcommittees
- **“Clinic of Clinics”** student networking and tabletop exercise each semester
- Active cybersecurity clinics **education and resource hub**
 - Syllabi, legal policies, client questionnaires

Clinic Foundation

4 Key Ingredients



**The Consortium of
Cybersecurity Clinics**

A Good Foundation: 4 Things You Need

1

Committed
Leader(s) or
Champion(s)

2

Interdisciplinary
Institutional
Support







3

Strong,
Supported
Clinic
Vision

4

Local
Partners

Clinic Vision: Instruction and Delivery

Program instruction		Faculty-taught
		Faculty-advised, instructor-taught
		Mentor-supported
Clinic model		Class: clinics are taught as standalone classes, typically over a semester
		Capstone: a client consulting project is introduced in an existing class, with shorter engagements
		Club or Internship: clinics operate year-round and conduct long-term engagements and follow-ups

Clinic Curriculum

Vendor-Neutral, Competitive, Dynamic

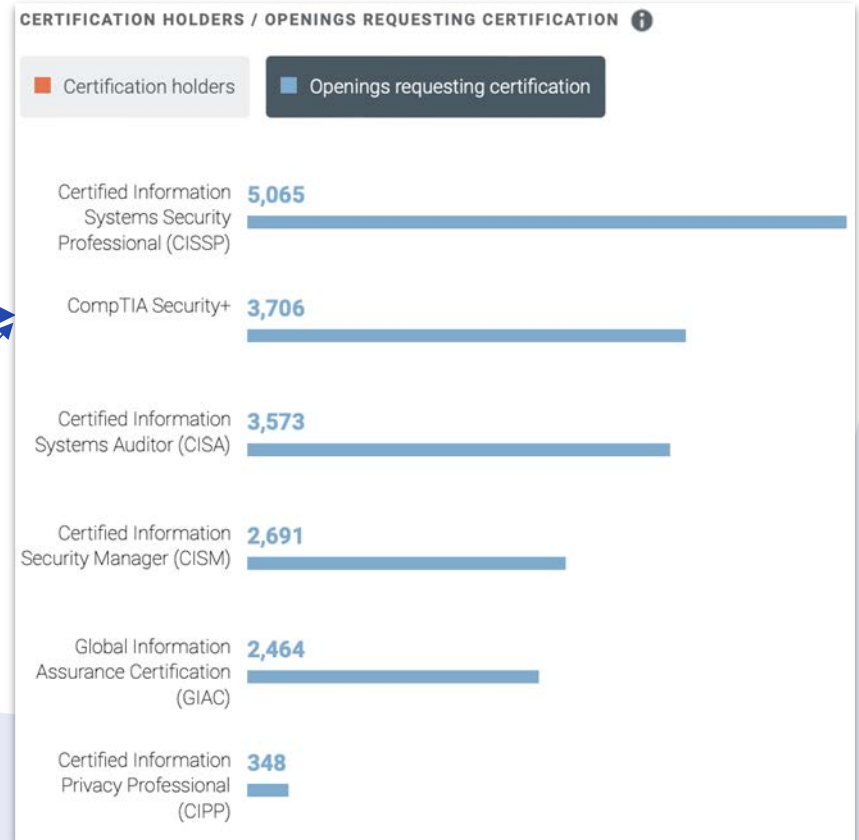
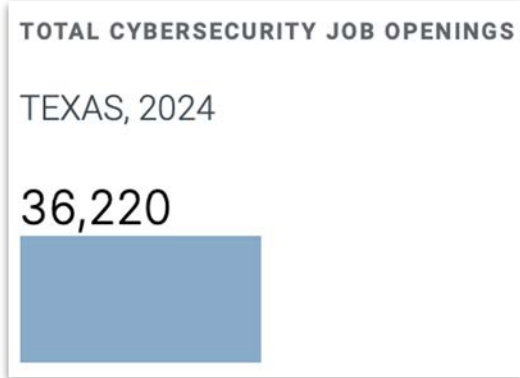


**The Consortium of
Cybersecurity Clinics**

What to Teach: Menu of Curricula and Services



What to Teach: Align With Industry Standards



What to Teach: Industry Standards

Grow with Google

Prepare for the CompTIA Security+ exam

The Google Cybersecurity Certificate helps prepare you for the CompTIA Security+ exam, the industry leading certification for cybersecurity roles. You'll earn a dual credential when you complete both.



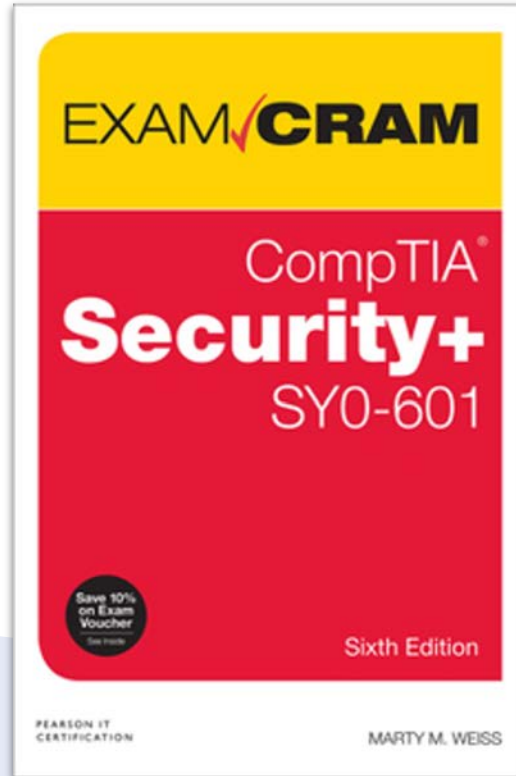
hands-on experience with Python, Linux, SQL, and more.

Get started at grow.google/cybersecurity

What to Teach: Industry Standards

Google Cybersecurity Certificate

to supplement student learning with a hands-on, professional development credential.



What to Teach: Industry Standards



CIS Controls

** The numbering system corresponds to specific Safeguards from the CIS Controls v8.0.*

- 2.3 Address Unauthorized Software
- 3.3 Configure Data Access Control Lists
- 3.4 Enforce Data Retention
- 4.1 Establish and Maintain a Secure Configuration Process
- 4.7 Manage Default Accounts on Enterprise Assets and Software
- 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts
- 6.3 Require MFA for Externally-Exposed Applications
- 6.4 Require MFA for Remote Network Access
- 6.5 Require MFA for Administrative Access
- 10.1 Deploy and Maintain Anti-Malware Software
- 10.2 Configure Automatic Anti-Malware Signature Updates
- 11.4 Establish and Maintain an Isolated Instance of Recovery Data

What to Teach: Industry Standards

- Identify
 - Asset Inventory
 - Risk Assessment*
- Protect
 - Encryption Schema
 - Password Management
 - Privacy Policies*
 - Authorization Management (Onboarding and Offboarding)
 - Vulnerability Scanning and Patching
 - Network, Wireless, Email, Mobile, and Cloud Security
 - Penetration Testing

What to Teach: Industry Standards

- Detect
 - AV and EDR Tools
 - IDSs, IPSs
 - SIEMs and SOAR
 - UTM Tools
- Respond
 - Incident Response Teams, Plans, and Tools*
 - Digital Forensics Basics
 - Compliance and Reporting Requirements*
- Recover
 - Business Continuity Planning*
 - Controls Modifications*

What to Teach: Power Skills

- Organization
 - Project planning
 - Report writing
- Communication
 - Simplify technical jargon
 - Treat clients as partners; focus on awareness and education
- Briefing
 - BLUF
 - “So what?”
- Teamwork
 - Paired according to discipline
 - Graded based on equal, regular contribution to project plan and tasks

Sample “Choose Your Own Adventure” Assignments

- Communication Skill Building
 - Pick a cybersecurity attack case study and, based on your group number, prepare to either **1) submit a written summary** or **2) brief the class** on the attack type, attack vector, and recommended mitigation to prevent the attack in the future.
- Technical Skill Building
 - **Foundational:** Complete the “Automate Cybersecurity Tasks with Python” course from the Google Cybersecurity Professional Certificate
 - **Intermediate:** Complete “Pentesting Fundamentals” and “Metasploit: Introduction” modules on TryHackMe

Clinic Funding and Kickoff

Identifying, Creating, and Sustaining Clinic Funding

- The cost of clinic startup and operations depends on your choice of instruction and delivery model, faculty/teachers, materials, enrollment, and support staff
 - Consortium clinics have found that **\$300k is a good funding target** for the first year, and **\$100k each year thereafter**
- After the first four to five years, clinics can blend their budgets with the host institution budget



Typical Clinic Budget Line-Items

Here are some typical line items for a clinic budget:

- Faculty and instructor paid time for the clinic, can include summer salary
- Graduate researcher / TA / Post-doc for clinic teaching assistance (often 1 TA per semester)
- Equipment: Laptops and security keys, software for analysis, secure storage and collaboration
- Curriculum development expenses
- (Optional) Student travel to meet with clinic clients in person
- (Optional) Budget for student travel to conferences
- (Optional) Time with institution's communications staff to raise awareness, recruit students, celebrate clinic successes
- (Optional) Paying students as interns

Clinic Kickoff

- It can take around **9 months to plan for a clinic launch**, including developing internal training, policies, and curricula
- Many clinics choose to run a **pilot program** with a small cohort of students to test and improve the clinic operations and curriculum

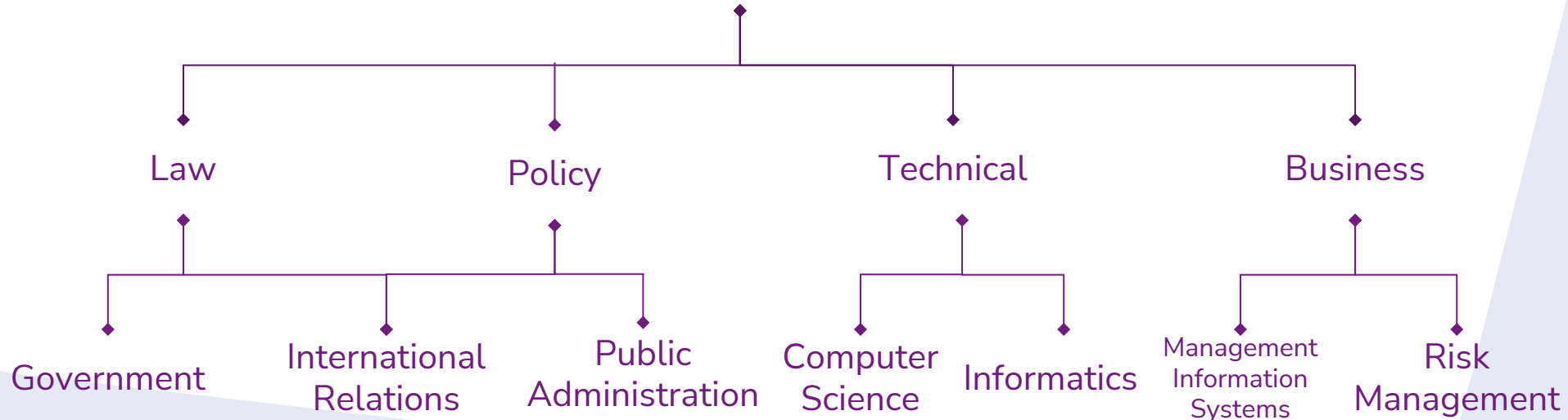


Student & Client Recruitment

Interdisciplinary, Diverse, Targeted,
High-Impact Industries

Clinic Students: Interdisciplinary Recruitment

Cybersecurity: A Team Sport!



Clinic Students: Application and Vetting

Qualifications: Application

Résumé

Cover Letter

GPA Minimum

Degree Progress

Aptitude: Interview

Prior Cybersecurity
Experience

Public Speaking &
Briefing

Writing & Research

Organization &
Leadership

Graphic Design

Vetting: Post- Interview

References

Letter(s) of
Recommendation

Background Check

Signed Code of
Conduct

Signed NDA

Clinic Governance: Policies, Indemnification, and Student Code of Conduct



CLINIC INTERNAL DATA GUIDANCE



Acceptable Use Policy

As a member of the MIT Cybersecurity Clinic, I will abide by the following policies and standard practices at all times during participating in the Clinic and having any access to clinic materials or environments.

Citizen Clinic Student Code of Conduct

The Citizen Clinic is an inclusive course where students, mentors, and staff should feel comfortable sharing their work, opinions, and perspectives. All of us commit to engaging with each other mindfully to ensure an environment that promotes shared learning and collaboration.



ROCHESTER INSTITUTE OF TECHNOLOGY AGREEMENT WITH COMPANY CORPORATION FOR THE STUDENT COURSE PROJECT

Clinic Clients: One or More Types

Clients to serve



Public entities: municipalities, hospitals, schools, libraries



Nonprofits: food banks, refugee organizations, health clinics



Small businesses: dentists, mom 'n pop shops



Blend: two or more types of clients

Connecting with Clinic Clients

Leverage Local Industry Organizations

- Chambers of Commerce
- Small Business Development Councils
- Councils of Government
- Association of Counties
- Nonprofit Professionals Network
- Local IT Professionals Network

Leverage College/University Connections

- Alumni Business Network
- Local Partnerships and City Offices
- Student Volunteer Groups and Partner Organizations
- Student Consulting Organizations



Clinic Learning & Impact

Client and Student Questionnaires



**The Consortium of
Cybersecurity Clinics**

Clinic Learning and Impact

Questionnaire for Students

- Reasons for participation
- Confidence and interest level regarding job prospects in cybersecurity
- Confidence in handling cybersecurity scenarios and communication

Questionnaire for Clients

- Reasons for seeking assistance
- Goal achievement evaluation
- Implementation of controls within their organization

Summary

Takeaways

- **Clinic Foundation**
 - Committed, well-positioned champion
 - (Interdisciplinary) institutional support
 - Strong, articulate, well-supported clinic vision
 - Local partners to identify clients
- **Clinic Instruction**
 - Map onto existing, well-known frameworks
 - Align with vendor-neutral and highly sought industry certifications
 - Incorporate group work, requiring “soft” skills to simulate real environment
 - Collaborate with Consortium of Cybersecurity Clinics for templates
- **Clinic Funding**
 - Corporate sponsors, donors, and philanthropies
 - University Departments or Centers
 - Local sponsors and fundraisers

Takeaways

- **Clinic Students**
 - Target interdisciplinary mix of degree programs and interests
 - Maintain ratio between undergraduate and graduate, technical vs. non-technical
 - Vet and assess capabilities and commitment to “real-world” clinic work
- **Clinic Clients**
 - Target industry appropriate to your institutional placement
 - Rely on local aggregate organizations, networks
 - Leverage existing local and college/school/university connections
- **Clinic Learning, Impact, and Growth**
 - Measure client maturity and confidence pre- and post-engagement
 - Measure student learning and workforce development pre- and post-services
 - Extrapolate and refine for long-term success and sustainment

Cyber Clinic Long-Term Outcomes

1

Provide **experiential education** and **skill-building** improving critical public infrastructure cybersecurity

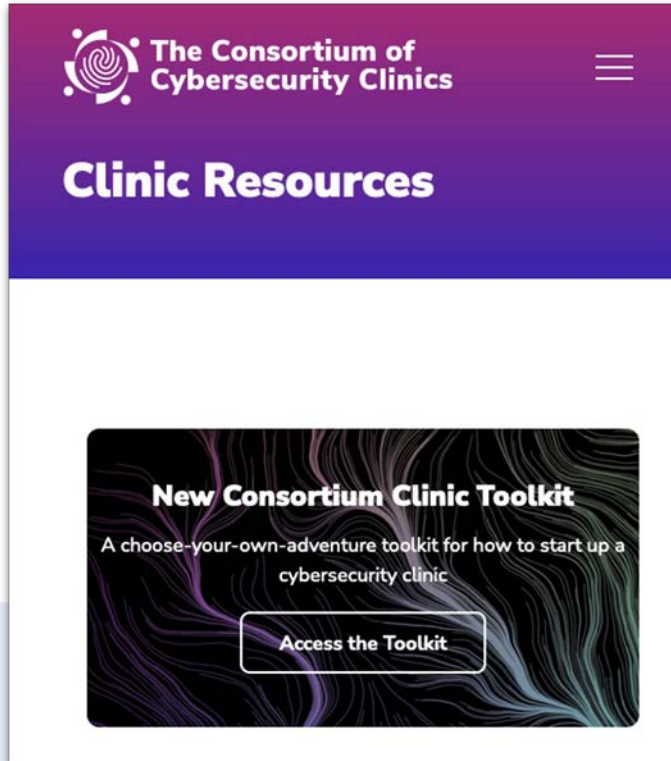
2

Improve **regional cyber** defensive posture, local **cyber education**, and **community resilience** to cyber attacks

3

Encourage **workforce development** and networking via mentors, experts, and sponsors

Cyber Clinic Development Resources



Read the full version of
our **Clinic
Development Toolkit:**
cybersecurityclinics.org

Q&A

Francesca Lockhart

Francesca.Lockhart@austin.utexas.edu

strausscenter.org

cybersecurityclinics.org



SCAN ME