The University of Texas at Austin
Strauss CENTER
for International Security and Law

The University of Texas at Austin
School of Computing

The University of Texas at Austin
Texas Cybersecurity Clinic

The Texas Cybersecurity Clinic at UT Austin is a two-semester, learn-then-do experience where student teams provide free cybersecurity services to Texas-based small businesses, public agencies, and nonprofits. The Clinic:

- Designs and renders customized cybersecurity improvement project plans for client organizations.
- Provides UT Austin undergraduate and graduate students with hands-on field-tested cybersecurity experience, helping them pursue careers in cybersecurity, national security, and related fields.
- Leverages the strong tradition of cybersecurity leadership at UT Austin to foster cyber resilience throughout Texas.

The Texas Cybersecurity Clinic consists of two, 3-credit hour courses hosted by the UT Austin School of Computing.

- **FOUNDATIONAL COURSE:** Students learn key cybersecurity defense best practices—including asset inventory, risk assessment, access control, network, cloud and AI security, incident response, and security policymaking—and practice the skills required to implement these concepts effectively in a real institutional setting.
- **PRACTICUM COURSE:** Students provide free cybersecurity hygiene services to their assigned client under the supervision of Professor Francesca Lockhart of the Strauss Center and with mentorship from expert cybersecurity practitioners.

Students work in teams of 3-4 to render services for a small number of clients each semester. Strong client candidates are critical infrastructure organizations with under 250 employees and little to no formal cybersecurity program or support. No prior cybersecurity knowledge or experience is required of the client team.

- **PROCESS:** Students first work with their client organization to develop a cybersecurity improvement project plan with a timeline spanning the service semester. Students then work with client organization staff to implement the project plan and provide the necessary education, training, and resources for continued management.
- **SERVICES:** Services are highly customizable depending on the short- and long-term needs and goals of the client organization. Sample services include, but are not limited to: identifying and evaluating assets and their criticality, configuring devices and software securely, creating organizational security policies, conducting custom cybersecurity education and awareness training, and developing incident response plans.

Strauss Center for International Security and Law | The University of Texas at Austin
www.strausscenter.org

francesca.lockhart@austin.utexas.edu

@STRAUSSCENTER

The University of Texas at Austin
Texas Cybersecurity Clinic

LEARN MORE

CLINIC SERVICES CAN INCLUDE, BUT ARE NOT LIMITED TO:

- **CYBER RISK ASSESSMENT:** Students identify, analyze, and evaluate potential threats and vulnerabilities to the client organization to determine the overall risk level of specific cyber threats. Students then use this assessment to create a detailed implementation plan and timeline to adopt high priority security controls over the rest of the semester.

- **ASSET INVENTORY:** Students identify and document systems and digital assets at the client organization, providing a robust record of all hardware, software, data, and accounts in use. This inventory is then tracked and maintained by the client long-term to manage cyber risk through visibility.

- **POLICY CREATION:** Based on the client's existing security program, policies, and any regulatory or legal requirements, students draft detailed policies covering areas such as password creation and storage, AI use, data protection, access control, etc. These policies provide clear instructions for personnel to maintain security across the organization.

- **SECURITY SOFTWARE CONFIGURATION:** Based on risk assessment findings, specific security controls—such as MFA, endpoint detection and response tools, and access management solutions—are implemented to bolster the client's cyber defenses. Students provide training and documentation to monitor and maintain the security controls.

- **INCIDENT RESPONSE PLANNING:** Based on the client organization's structure and roles, students draft a plan which outlines the roles, responsibilities, and procedures that personnel must follow during a cyber incident to report problems, minimize damage, recover quickly, and prevent future occurrences.

- **CUSTOMIZED CYBER TRAINING AND AWARENESS:** After an assessment of the client organization's current security awareness levels, students educate employees about cybersecurity best practices and the importance of maintaining a secure digital environment. Topics include recognizing phishing attempts, creating strong passwords, safe internet browsing, responsible and secure AI use, and responding to security incidents.

- **RECOMMENDATIONS FOR ADVANCED SERVICES, TRAININGS, AND RESOURCES:** Client organizations looking for more help or to continue their security momentum can ask students to assess cybersecurity products or service providers for their suitability. The students' findings are compiled into a detailed report which provides recommendations for the best-fit solutions. Students thus help ensure the organization selects a cybersecurity product or provider that meets current needs and supports its future security strategy and objectives.

Strauss Center for International Security and Law | The University of Texas at Austin
www.strausscenter.org

francesca.lockhart@austin.utexas.edu

@STRAUSSCENTER