



Jen Easterly, Director of CISA



Cybersecurity Clinic Students



Harry Kresja, Assistant National
Cyber Director



Applied Cybersecurity Community Clinic

Free Cyber Capacity-Building for
Local Governments

Francesca Lockhart

Francesca.Lockhart@austin.utexas.edu
strausscenter.org



The Strauss Center integrates expertise from across the University of Texas at Austin, as well as from the private and public sectors, in pursuit of practical solutions to emerging national and international challenges.



Applied Cybersecurity Community Clinic



Enhancing Community Cybersecurity
and Training Future Texas Cyber Leaders

UT Cyber Clinic Students



Step 1: Learn cyber defense fundamentals

Step 2: Work with local organizations to improve their cybersecurity



Fall 2023: 19 students

- Risk assessment
- Vulnerability management
- Secure network configuration
- Access control frameworks
- Business planning

Spring 2024: 5 clients

- 2 small businesses
- 1 faith-based nonprofit
- 2 city governments
- 18 new students

Fall 2024: 6 clients

- Up to 32 new students



Wendy Nather, Head of Advisory CISOs at Cisco

Key Outcomes

- Experiential education improving critical public infrastructure cybersecurity
- Improved regional defensive posture, cyber educational opportunity, and community resilience
- Workforce development and networking via Industry Expert Mentors and Corporate Sponsors



UT Cyber Clinic Students

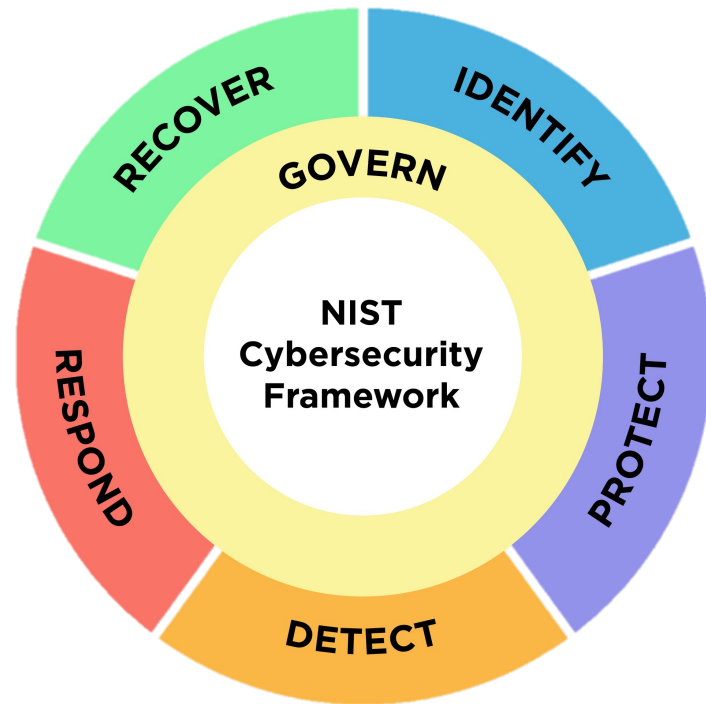
What We Teach: Industry Standard

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



* = Governance, Risk, and Compliance

What We Teach: Industry Standard

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*










* = Governance, Risk, and Compliance

Executive Summary:

Following an extensive risk assessment for Ballot’s Bowwow Box (BBB), we were pleased to see some individual security measures, including 2FA, backups, and password manager use. Any pre-existing cybersecurity measures already in place act as a good foundation to build upon on an organizational level.

However, we have identified various critical risks, high risks, moderate risks, low risks, and negligible risks in your company’s infrastructure. These risks pose immediate threats to the company’s safety and integrity, and we advise that action is taken swiftly. Most of these risks have affordable solutions, and all solutions recommended will take within four months to implement, with room for flexibility.

Risk	Vulnerabilities
	Lack of Physical Security in Co-Working Space Regarding Printer and Device Access
	Lack of Firewall
	Systemic Lack of Two-Factor Authentication
	Lack of VPN Usage
	Lack of Distinction Between Usage of Company and Personal Devices and Data
	Devices and Software are Out-of-Date
	Lack of Incident Response Plan

Impact				
Likelihood		Low	Medium	High
	High	Moderate	High	Critical
	Medium	Low	Moderate	High
	Low	Negligible	Low	Moderate

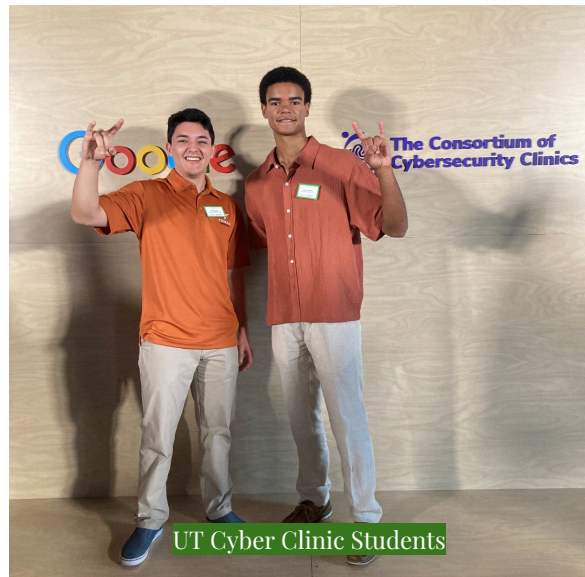
Detect				
Control	Priority	Suggested or Required Tool	Control Type and Explanation	Cost
Unsuccessful Login Attempt Detection	Critical	Cloud-based IAM solution (Auth0, Google Cloud Identity, firebase, auth.js)	Technical – enabling login attempts for accounts (external services) that have security features can give visibility into attempts.	Free/Ranges based on active users (Ex: Auth0 - 5,000 active monthly users for B2C would cost >\$350 monthly to implement)
DMARC, DKIM, SPF Enabled	Critical	Google Workspace	Technical – these email authentication standards can be configured in Google Admin Console. A an easy, impactful solution to prevent email spoofing/phishing	Free/included when choosing Google Workspace
Logging and Monitoring	High	Google Workspace, External services may have security features built-in, Cloud-based IAM solutions (Auth0...)	Technical – reviewing failed logins/unusual patterns in activity in conjunction with the Unsuccessful Login Attempt Detection	Free/Ranges based on active users (Ex: Auth0 - 5,000 active monthly users for B2C would cost >\$350 monthly to implement)



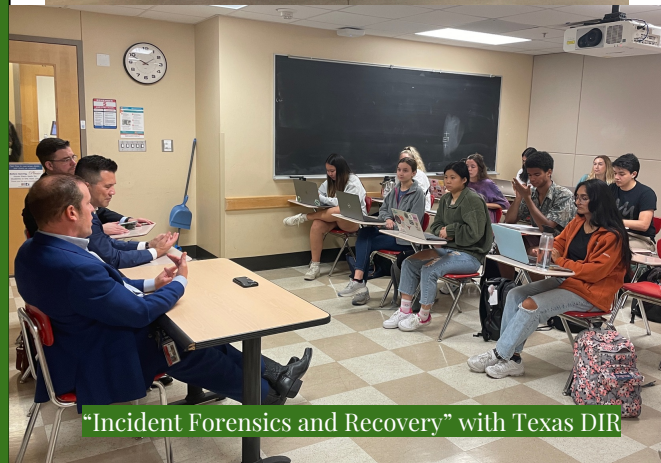
"Cyber Law" with Associate General Counsel for
Cybersecurity (NSA)

Get Involved

- Become a client, or refer an organization
 - We can partner with individual COGs as force multipliers, or work with a city within your COG in need of services
- Host interns or share job openings with clinic
 - All juniors and seniors
- Guest lecture, or serve as an Industry Expert Mentor
 - 1 hour class, or work with a student team 1 hour/week



UT Cyber Clinic Students



"Incident Forensics and Recovery" with Texas DIR

The background of the slide is a nighttime photograph of the UT Tower in Austin, Texas, illuminated with warm orange and red lights. In the foreground, a large fountain with multiple jets of water is lit up, creating a misty spray. The scene is dark, with the lights from the tower and fountain providing the primary illumination.

Francesca Lockhart

Francesca.Lockhart@austin.utexas.edu

strausscenter.org

cybersecurityclinics.org



LEARN MORE

Q&A