Essentials of Community Cybersecurity
AWR136

FEMA

- 67% of companies with critical infrastructure suffered at least one attack in the past 12 months.
- 78% expect a successful exploit of their ICS/SCADA systems within the next two years.
- 91% of power generation organizations have experienced a cyber attack.
- 61% believe it’s unlikely they would be able to detect a sophisticated attack.
- 51% have not deployed technology to detect or prevent advanced persistent threats.

What is Cyber?

Cyber Definition

"Anything that contains, is connected to, or controlled by computers and computer networks."

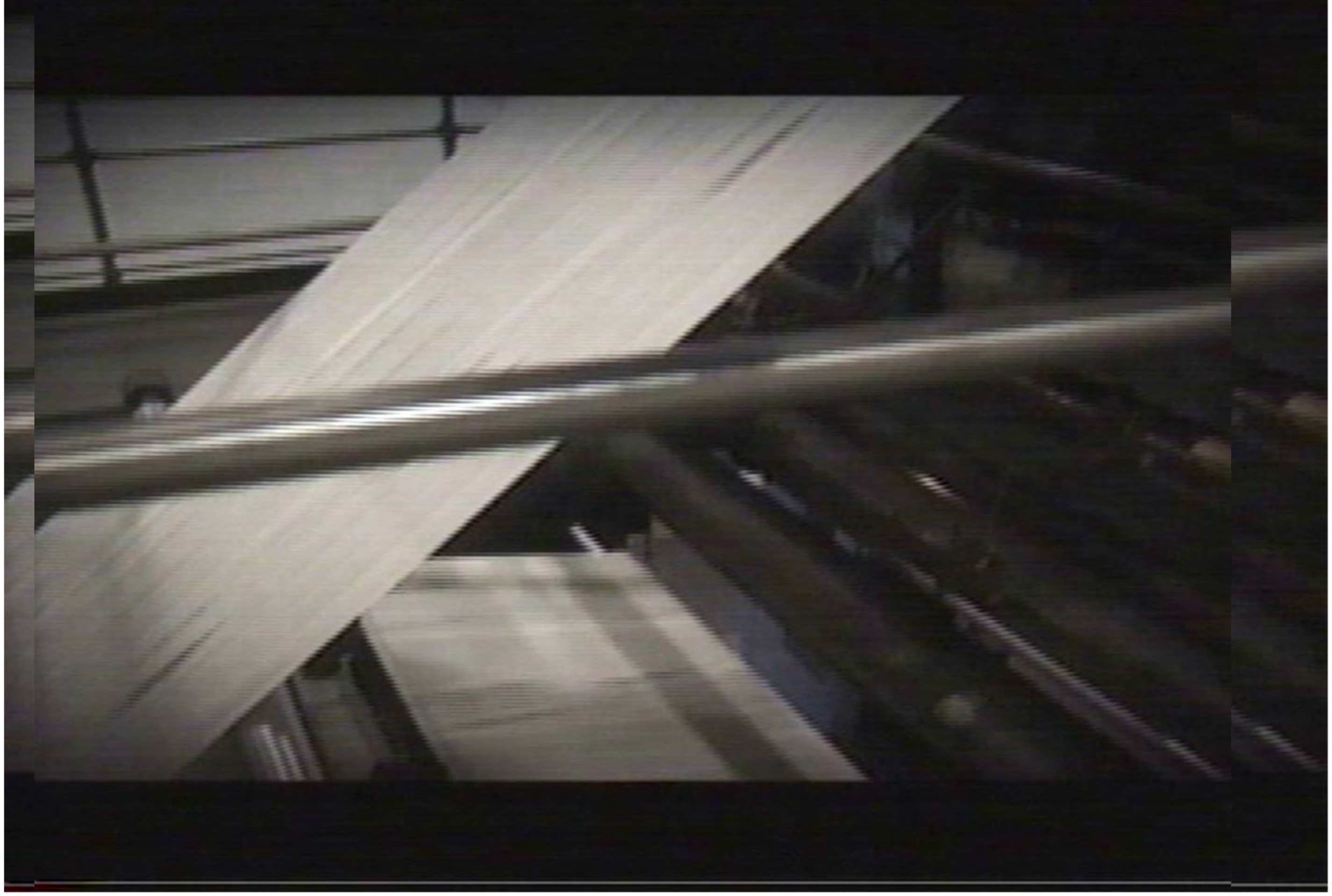
What Does Cyber Mean to You?

Critical Infrastructure

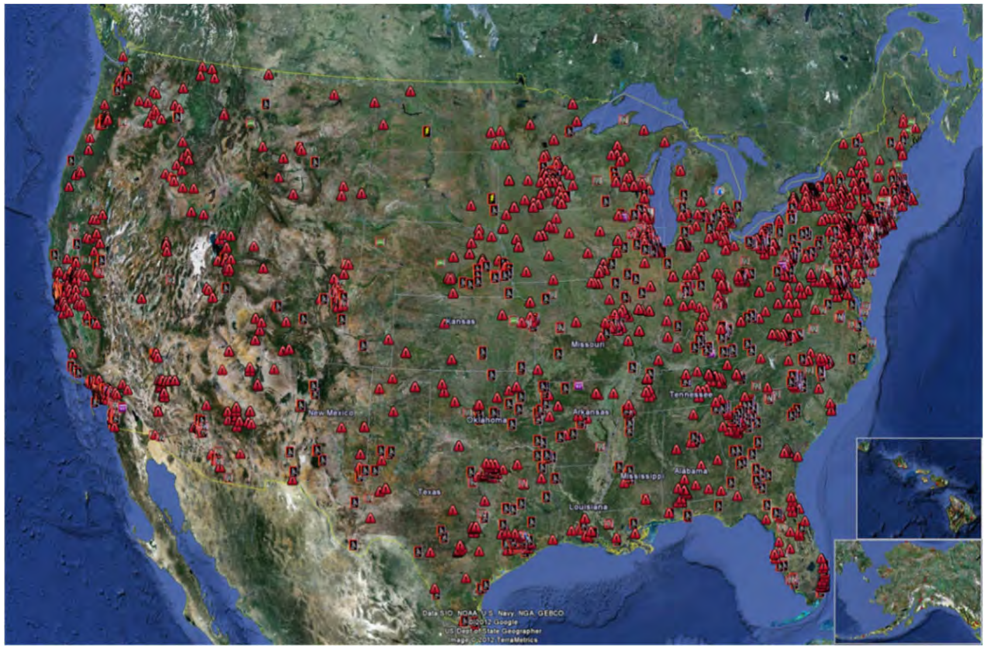
Cyber Security

The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)

PBS Special “Cyber War”



Publicly Accessible Critical Infrastructure

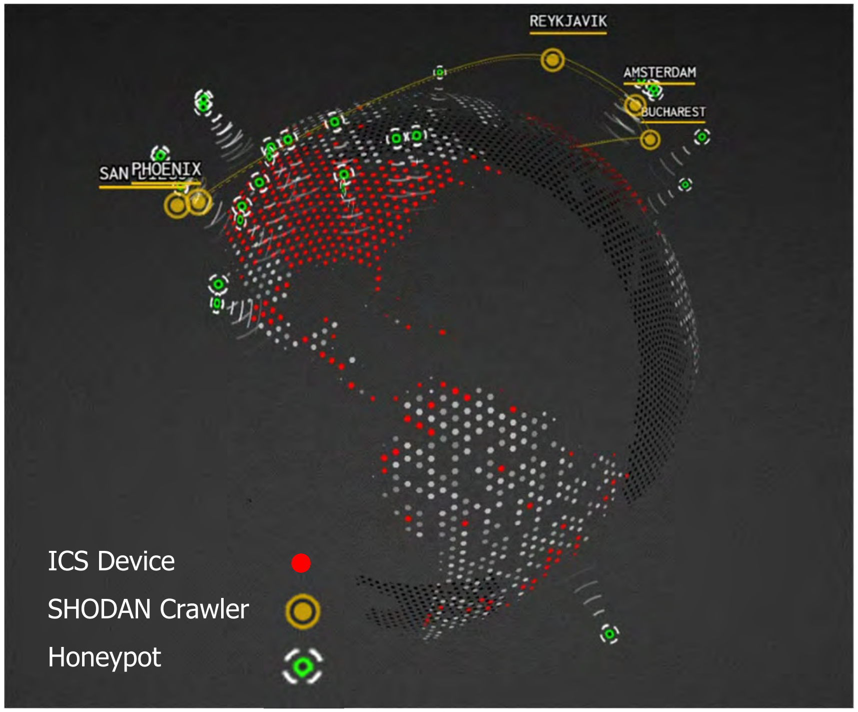


- 7000+ Publicly Accessible SCADA / DCS systems
- “In some instances, these devices have either weak, default, or nonexistent logon credential requirements. “
- “Once accessed, these devices may be used as an entry point onto a control systems network, making their Internet facing configuration a major vulnerability to critical infrastructure.”

Source: ICS-CERT, December 2012

SHODAN

- www.shodanhq.com
- Identify IP addresses regardless of the type of device
- Identify SCADA systems

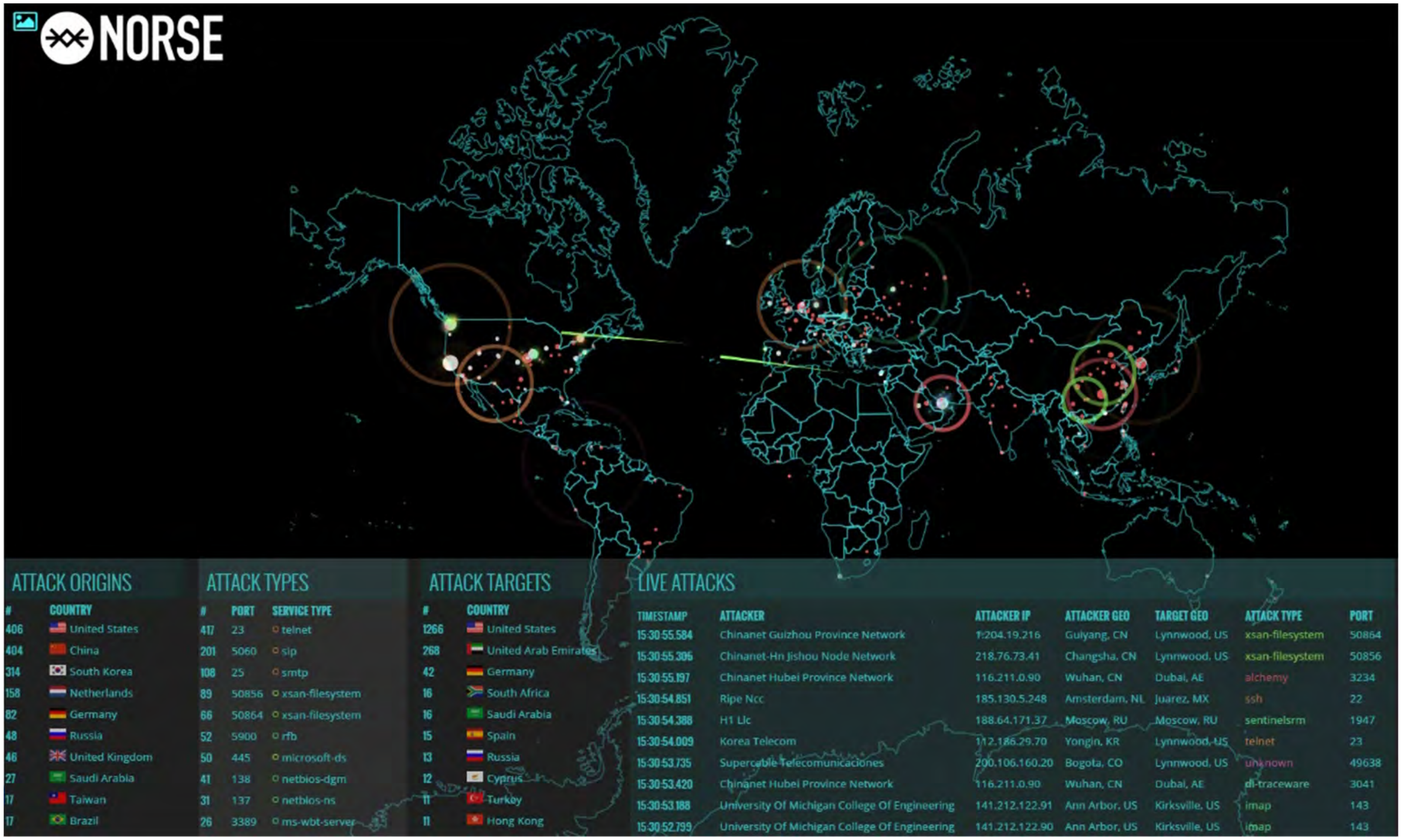


The Shodan search engine has started to crawl the Internet for protocols that provide raw, direct access to industrial control systems (ICS). This visualization shows the location of these industrial control systems on the Internet as well as other related data. https://ics-radar.shodan.io/

Module 2: Cyber Threats and Vulnerabilities

FEMA

The Global Threat



ATTACK ORIGINS

#	COUNTRY
406	United States
404	China
314	South Korea
158	Netherlands
82	Germany
48	Russia
46	United Kingdom
27	Saudi Arabia
17	Taiwan
17	Brazil

ATTACK TYPES

#	PORT	SERVICE TYPE
417	23	telnet
201	5060	sip
108	25	smtp
89	50856	xsan-filesystem
66	50864	xsan-filesystem
52	5900	rfb
50	445	microsoft-ds
41	138	netbios-dgm
31	137	netbios-ns
26	3389	ms-wbt-server

ATTACK TARGETS

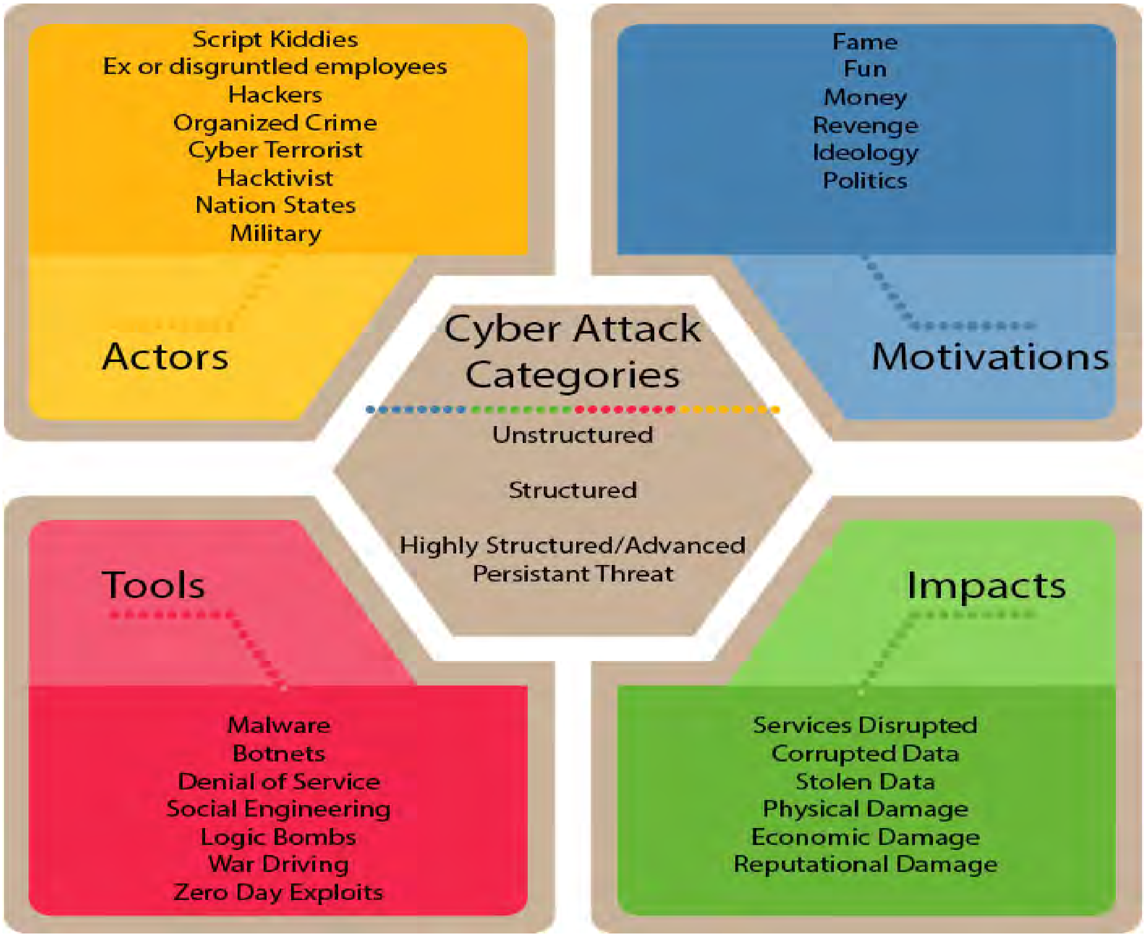
#	COUNTRY
1266	United States
268	United Arab Emirates
42	Germany
16	South Africa
16	Saudi Arabia
15	Spain
13	Russia
12	Cyprus
11	Turkey
11	Hong Kong

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
15:30:55.584	Chinanet Guizhou Province Network	1:204.19.216	Guiyang, CN	Lynnwood, US	xsan-filesystem	50864
15:30:55.306	Chinanet-Hn Jishou Node Network	218.76.73.41	Changsha, CN	Lynnwood, US	xsan-filesystem	50856
15:30:55.197	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	alchemy	3234
15:30:54.851	Ripe Ncc	185.130.5.248	Amsterdam, NL	Juarez, MX	ssh	22
15:30:54.388	H1 Llc	188.64.171.37	Moscow, RU	Moscow, RU	sentinelsrm	1947
15:30:54.009	Korea Telecom	112.186.29.70	Yongin, KR	Lynnwood, US	telnet	23
15:30:53.735	Supercable Telecomunicaciones	200.106.160.20	Bogota, CO	Lynnwood, US	unknown	49638
15:30:53.420	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	di-traceware	3041
15:30:53.188	University Of Michigan College Of Engineering	141.212.122.91	Ann Arbor, US	Kirksville, US	imap	143
15:30:52.799	University Of Michigan College Of Engineering	141.212.122.90	Ann Arbor, US	Kirksville, US	imap	143

Norse Live Attack Map

Contributing Factors



Examples of Unstructured Threat

- Malware
- Removeable Media
- Phishing/ Smishing/ Vishing
- Drive-by Downloads
- Public Wi-Fi
- War Driving

Dangers of WiFi

Types of Structured Attacks

- Social Engineering
- Botnets
- Distributed Denial of Service (DDoS)
- Zero Day Exploits

—AND use of unstructured attacks

Social Engineering

- The practice of obtaining confidential information by manipulation of legitimate users
  - E-mail
  - Telephone
  - Face-to-Face
  - Shoulder Surfing
  - Dumpster diving
  - Spear Phishing/ Smishing/ Vishing
    - Whaling
  - Insider Threat
  - Social Networking Sites

- **Phishing** – fraudulent practice of sending emails in order to trick people into sending personal information.
  - **Spear-Phising** – The same as phishing but appears to come from a trusted source *i.e. banking , credit cards, etc.*
  - **Whaling** – phishing technique that targets executives and top officials of organizations and companies.
- **SMShing** – texting version of phishing.
- **Vishing** – fraudulent practice of making phone calls in order to induce individuals to reveal personal information *i.e. banks or organizational details*
- **WIFI** – Acts as the man-in-the-middle collecting your personal info.
- **Dumpster Diving** – Looking through trash for sensitive information.
- **Shoulder Surfing** – Watching keys you press when entering passwords.
- **Face-to-Face** – Gathering enough information from research to engage in face-to-face conversation to gain sensitive information.

- **Neuro-Linguistic Hacking – The Twelve Laws**

1. **Dissonance** – Gravitate to people who are consistent in their behavior.
2. **Obligation** – When people do for us, stronger need to return the favor.
3. **Connectivity** – The more connected to, liked by, attracted to, the more influential you become. 4 factors: attraction, similarity, people skills, rapport.
4. **Social Validation** – Desire to belong and be accepted.
5. **Scarcity** – Supply and demand situations.
6. **Verbal Packaging** – Use easy, respectful language that's captivating.
7. **Contrast** – Introducing two vastly different alternatives in succession.
8. **Expectations** – If expectation is laid out usually they comply.
9. **Involvement** – Engage the 5 senses mentally & physically creates right atmosphere to be influenced i.e. grocery stores.
10. **Esteem** – The need & want to be praised, recognized and accepted.
11. **Association** – Our brains link objects, gestures, symbols with feelings & memories, and life experiences.
12. **Balance** – Balance both the logical and emotional for perfect persuasion.

Who’s the Weakest Link?

- Social engineering cares less about how strong:
  - Firewalls
  - Intrusion Detection Systems
  - Anti-virus software
  - Cybersecurity posture

- The **HUMAN** factor is the weakest link.

As long as there are feelings in involved, humans are more vulnerable than computers.

SO WHAT CAN YOU DO?

- Have a PLAN in place to be able to:
  - Identify, Protect, Detect, Respond, Recover
  - Good Policies and Procedures
  - **Training, Training, Training** and did I mention **TRAINING!**
  - Information Sharing

PASSWORDS!!!

Passwords

TEXAS A&M ENGINEERING

TEEX

EXTENSION SERVICE

Cybersecurity Courses

Program Overview

- 10 Online Cybersecurity Training Courses
- 7 Instructor-led Courses
- Custom Student Training Portal

Benefits of Online Courses

- Increase Cybersecurity Awareness
- Professional Development
- CEU Credit
- No Cost to Participants
- ACE College Credit Recommended

Online for Everyone – Non-technical 2 Credits

- AWR 168 – Cyber Law and White Collar Crime
- AWR 174 – Cyber Ethics
- AWR 175 – Information Security for Everyone

Business Professionals 2 Credits

- AWR 169 – Cyber Incident Analysis and Response
- AWR 176 – Business Information Continuity
- AWR 177 – Information Risk Management

IT Professionals – 2 Credits

- AWR 138 – Network Assurance
- AWR 139 – Digital Forensics Basics
- AWR 173 – Information Security Basics
- AWR 178 – Secure Software

General / Non-Technical Track

Introduces the basic principles and practices computer users need to keep themselves safe at work and at home. Intended for individuals new to information security, organizations looking to provide basic information security training for their employees or as a resource for college courses.

- Information Security for Everyone (AWR-175-W)
- Cyber Ethics (AWR-174-W)
- Cyber Law and White Collar Crime (AWR-168-W)

Technical / IT Professional Track

Focuses on methods individuals and organizations can use to secure computers, applications and networks and provides the basics of digital forensics. Perfect for individuals with technical knowledge of computers, operating systems and networks or with an interest in digital forensics

- Information Security Basics (AWR-173-W)
- Secure Software (AWR-178-W)
- Network Assurance (AWR-138-W)
- Digital Forensics Basics (AWR-139-W)

Business Professionals Track

Addresses implementation and management of an information security business continuity plan, managing risk and methods to keep systems safe from intrusion.

- Disaster Recovery for Information Systems (AWR-176-W)
- Information Risk Management (AWR-177-W)
- Cyber Incident Analysis and Response (AWR-169-W)

Instructor-led Courses

Awareness Level Classes

- AWR135-Promoting Community Cybersecurity
- AWR136-Essentials of Community Cybersecurity

Management Level Courses

- MGT384- Community Preparedness for Cyber Incidents
- MGT385-Community Cybersecurity Exercise Planning
- MGT452- Physical and Cyber Security for Critical Infrastructure

Management Level Courses

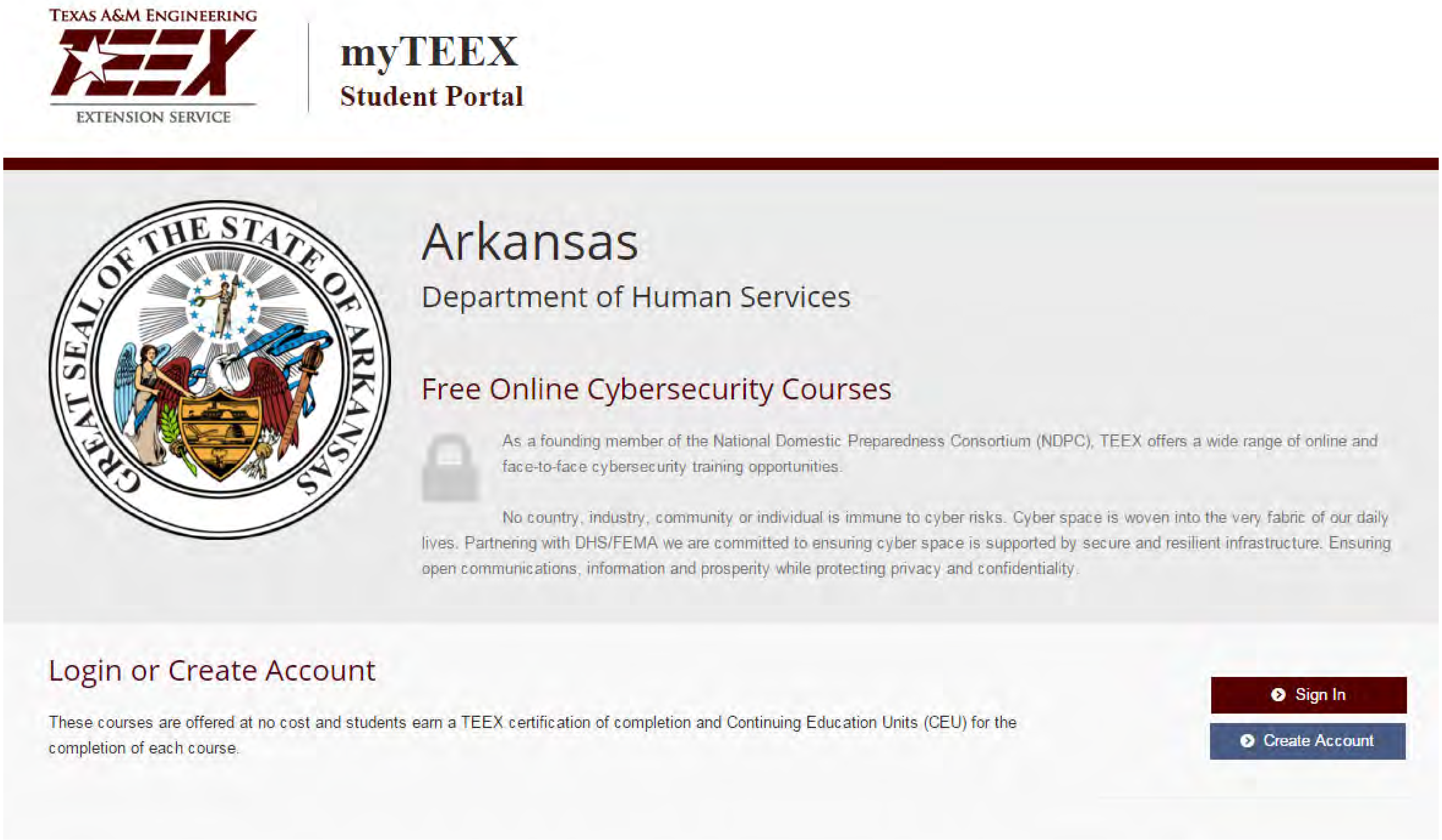
- MGT456- Integration of Cybersecurity Personnel into the Emergency Operations Center
- PER371-Cybersecurity Incident Response for IT Personnel

New and Coming Soon

- Recovering from Cyber Incidents (in pilot)
- Cybersecurity Awareness for Senior Officials
- Advanced Persistent Threats (APT)

Online Training Portal

Branded Landing Page



Texas A&M Engineering TEEX Extension Service

myTEEX
Student Portal

Arkansas

Department of Human Services

Free Online Cybersecurity Courses

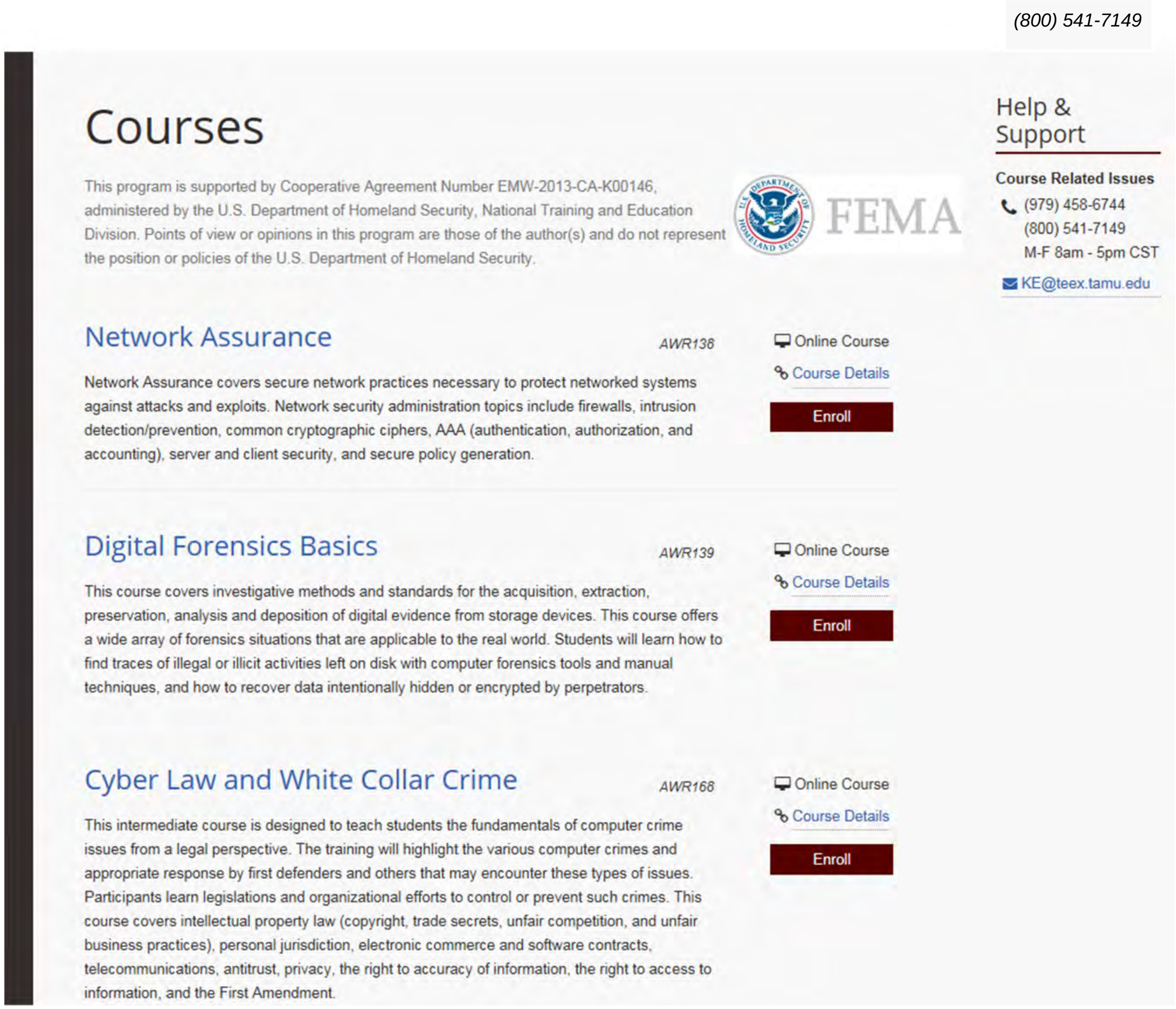
As a founding member of the National Domestic Preparedness Consortium (NDPC), TEEX offers a wide range of online and face-to-face cybersecurity training opportunities.

No country, industry, community or individual is immune to cyber risks. Cyber space is woven into the very fabric of our daily lives. Partnering with DHS/FEMA we are committed to ensuring cyber space is supported by secure and resilient infrastructure. Ensuring open communications, information and prosperity while protecting privacy and confidentiality.

Login or Create Account

These courses are offered at no cost and students earn a TEEX certification of completion and Continuing Education Units (CEU) for the completion of each course.

Custom Course Catalog



(800) 541-7149

Courses

This program is supported by Cooperative Agreement Number EMW-2013-CA-K00146, administered by the U.S. Department of Homeland Security, National Training and Education Division. Points of view or opinions in this program are those of the author(s) and do not represent the position or policies of the U.S. Department of Homeland Security.

Network Assurance

AWR138

Online Course

Course Details

Enroll

Network Assurance covers secure network practices necessary to protect networked systems against attacks and exploits. Network security administration topics include firewalls, intrusion detection/prevention, common cryptographic ciphers, AAA (authentication, authorization, and accounting), server and client security, and secure policy generation.

Digital Forensics Basics

AWR139

Online Course

Course Details

Enroll

This course covers investigative methods and standards for the acquisition, extraction, preservation, analysis and deposition of digital evidence from storage devices. This course offers a wide array of forensics situations that are applicable to the real world. Students will learn how to find traces of illegal or illicit activities left on disk with computer forensics tools and manual techniques, and how to recover data intentionally hidden or encrypted by perpetrators.

Cyber Law and White Collar Crime

AWR168

Online Course

Course Details

Enroll

This intermediate course is designed to teach students the fundamentals of computer crime issues from a legal perspective. The training will highlight the various computer crimes and appropriate response by first defenders and others that may encounter these types of issues. Participants learn legislations and organizational efforts to control or prevent such crimes. This course covers intellectual property law (copyright, trade secrets, unfair competition, and unfair business practices), personal jurisdiction, electronic commerce and software contracts, telecommunications, antitrust, privacy, the right to accuracy of information, the right to access to information, and the First Amendment.

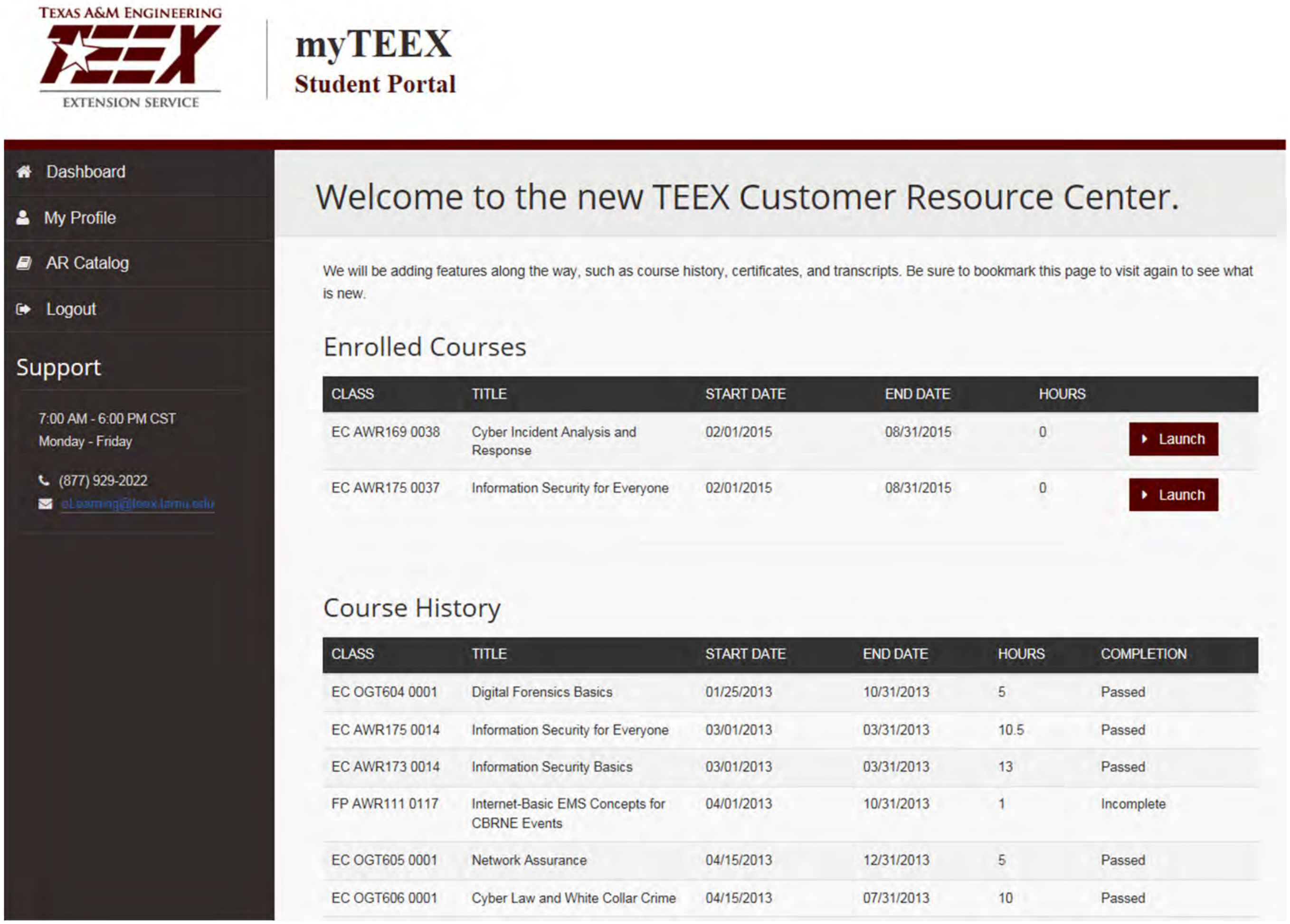
Help & Support

Course Related Issues

☎ (979) 458-6744
(800) 541-7149
M-F 8am - 5pm CST

✉ KE@teex.tamu.edu

Student Dashboard



TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

myTEEX
Student Portal

- Dashboard
- My Profile
- AR Catalog
- Logout

Support

7:00 AM - 6:00 PM CST
Monday - Friday

☎ (877) 929-2022
eLearning@teex.tamu.edu

Welcome to the new TEEX Customer Resource Center.

We will be adding features along the way, such as course history, certificates, and transcripts. Be sure to bookmark this page to visit again to see what is new.

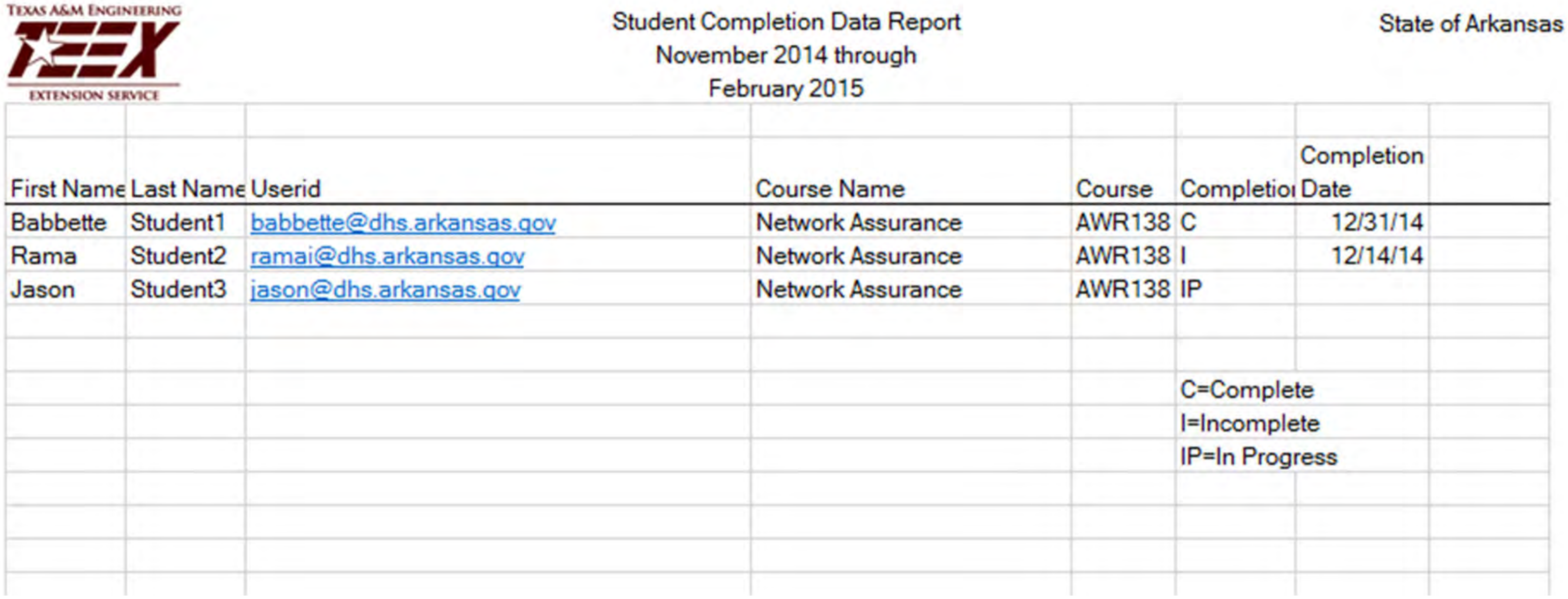
Enrolled Courses

CLASS	TITLE	START DATE	END DATE	HOURS	
EC AWR169 0038	Cyber Incident Analysis and Response	02/01/2015	08/31/2015	0	▸ Launch
EC AWR175 0037	Information Security for Everyone	02/01/2015	08/31/2015	0	▸ Launch

Course History

CLASS	TITLE	START DATE	END DATE	HOURS	COMPLETION
EC OGT604 0001	Digital Forensics Basics	01/25/2013	10/31/2013	5	Passed
EC AWR175 0014	Information Security for Everyone	03/01/2013	03/31/2013	10.5	Passed
EC AWR173 0014	Information Security Basics	03/01/2013	03/31/2013	13	Passed
FP AWR111 0117	Internet-Basic EMS Concepts for CBRNE Events	04/01/2013	10/31/2013	1	Incomplete
EC OGT605 0001	Network Assurance	04/15/2013	12/31/2013	5	Passed
EC OGT606 0001	Cyber Law and White Collar Crime	04/15/2013	07/31/2013	10	Passed

Monthly Tracking Report



TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

Student Completion Data Report
November 2014 through
February 2015

State of Arkansas

First Name	Last Name	Userid	Course Name	Course	Completio	Completion Date
Babbette	Student1	babbette@dhs.arkansas.gov	Network Assurance	AWR138	C	12/31/14
Rama	Student2	ramai@dhs.arkansas.gov	Network Assurance	AWR138	I	12/14/14
Jason	Student3	jason@dhs.arkansas.gov	Network Assurance	AWR138	IP	

C=Complete
I=Incomplete
IP=In Progress

Devalle Clay

Devalle.Clay@teex.tamu.edu

Carla Collins

Carla.Collins@teex.tamu.edu

979-458-6715

www.teex.org/cyber