A Review of Community Cybersecurity and Preparedness

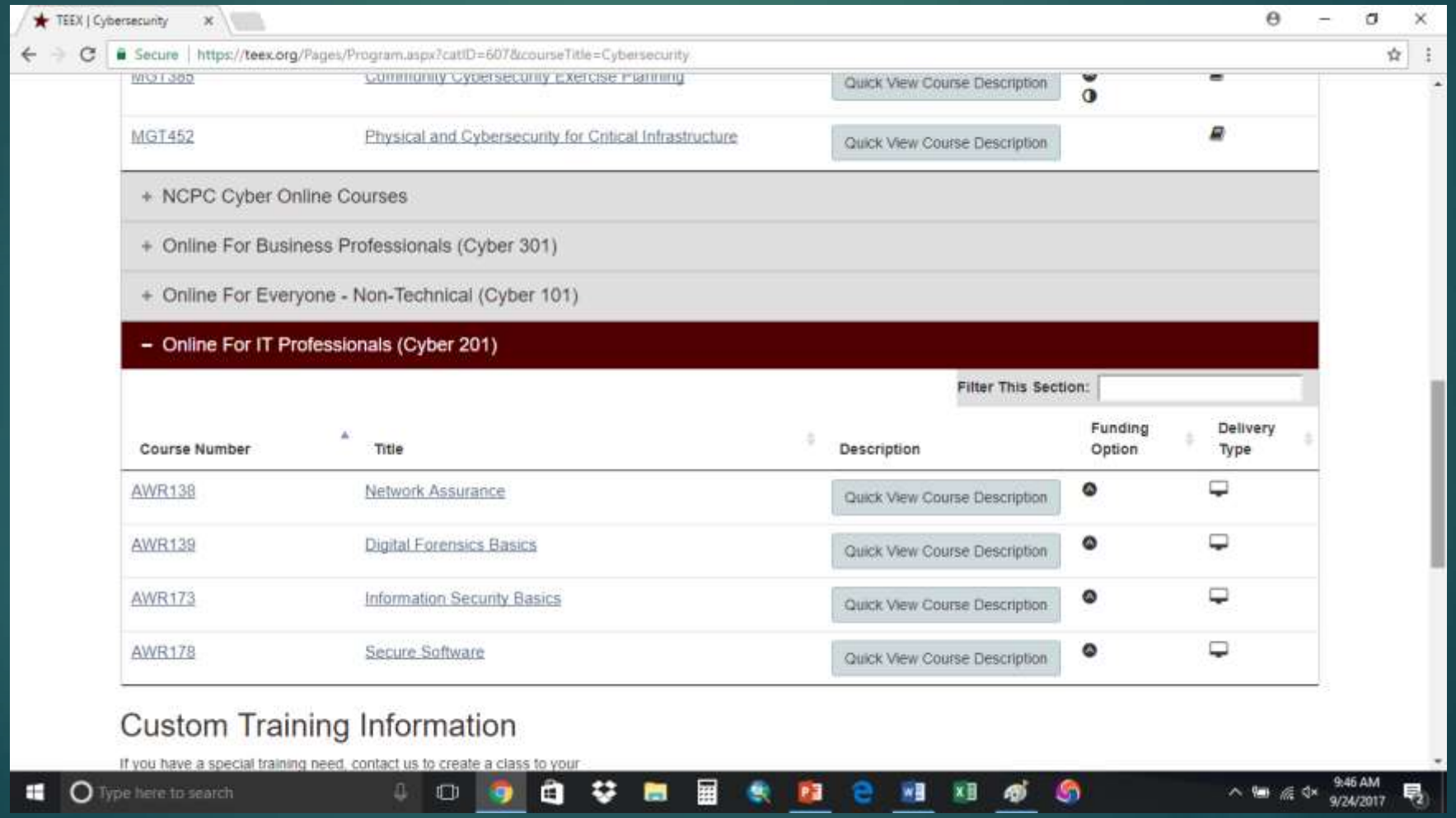
CARL L. ZIMMERMAN, PHD

CZIMMERMAN@WESTCOG.ORG

Training Provided by FEMA and TEEX

- Summary of two courses
  - Essentials of Community Cybersecurity
  - Community Preparedness for Cyber Incidents
- Not expert rather reporting results and possible next steps as a Region
- Goals: Summarize and spread training around to the Region
- Initiate discussion on whether there is interest in creating working group
- Free training if you can get 25 participants

TEEX (teex.org)



Overview

- Cyber incidents and attacks are **significant** threat to infrastructure, networks, and communities (especially smaller ones with less resources)
- Threats can come from individuals, organizations, nation-states – each has a variety of techniques
- An assessment of preparedness and baseline is important to understand threats and risks
- Community cybersecurity planning should be applied to these issues-- just like for other community threats (i.e. emergency management)
- We are introducing this topic to begin the discussion on what a Cybersecurity Task Force would look like in this region
- Resources are available

Definition of Cyber

- Cyber is anything connected, controlling or containing computers and computer networks
- Modern business and government processes totally embedded with cyber
  - Examples:
    - Email
    - Document management and human resources
    - GIS
    - Parcels and CAMA management
    - Accounting
    - Controllers for utilities and traffic signals

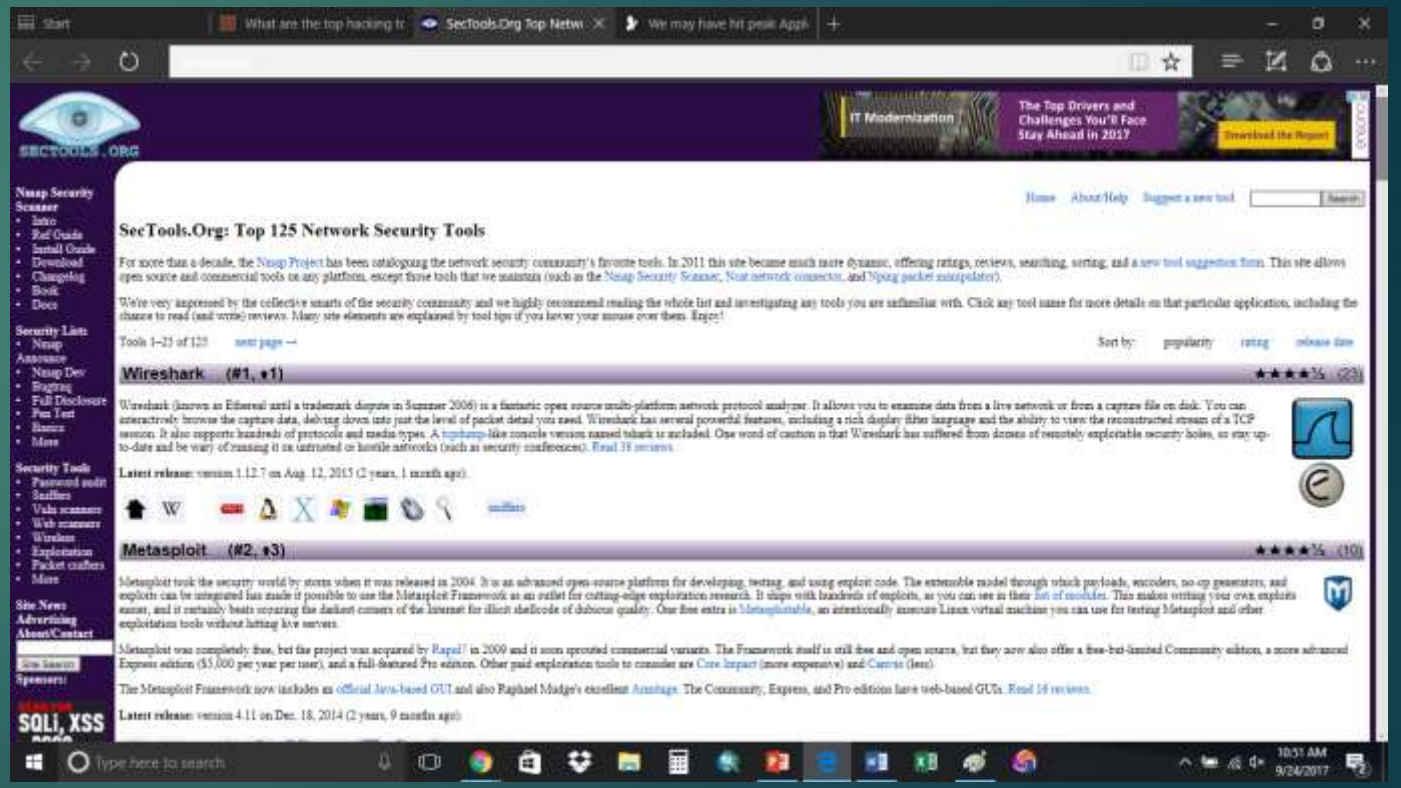
Critical Infrastructure Tied to Cyber

- Financial systems/ATM
- SAP and management systems
- Dams and water
- Power grid, nuclear reactor systems
- Rail and shipping
- Health Care and Public Health

Found at Washington Post: https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.0b06ab0228a0

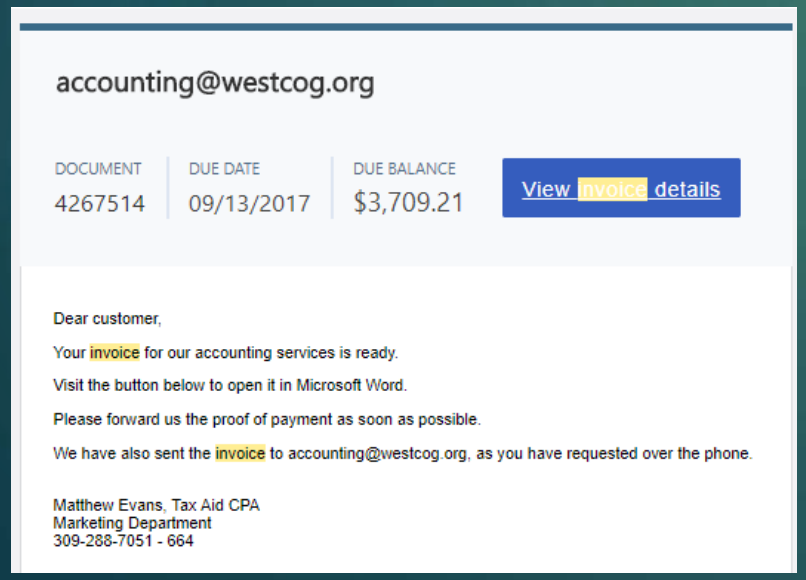
Three Types of Threats

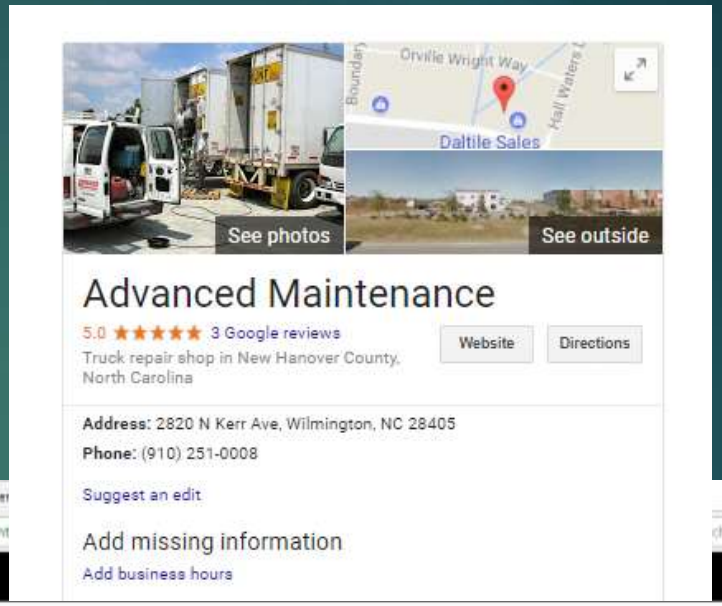
- Unstructured
  - Opportunists and utilize easily available tools (script kiddies)
- Structured
  - Higher degree of organization, planning, and "professionalism" (ex. Mob)
- Highly Structured
  - Nation-state sponsored or political organizations
  - Physical attacks and cyber

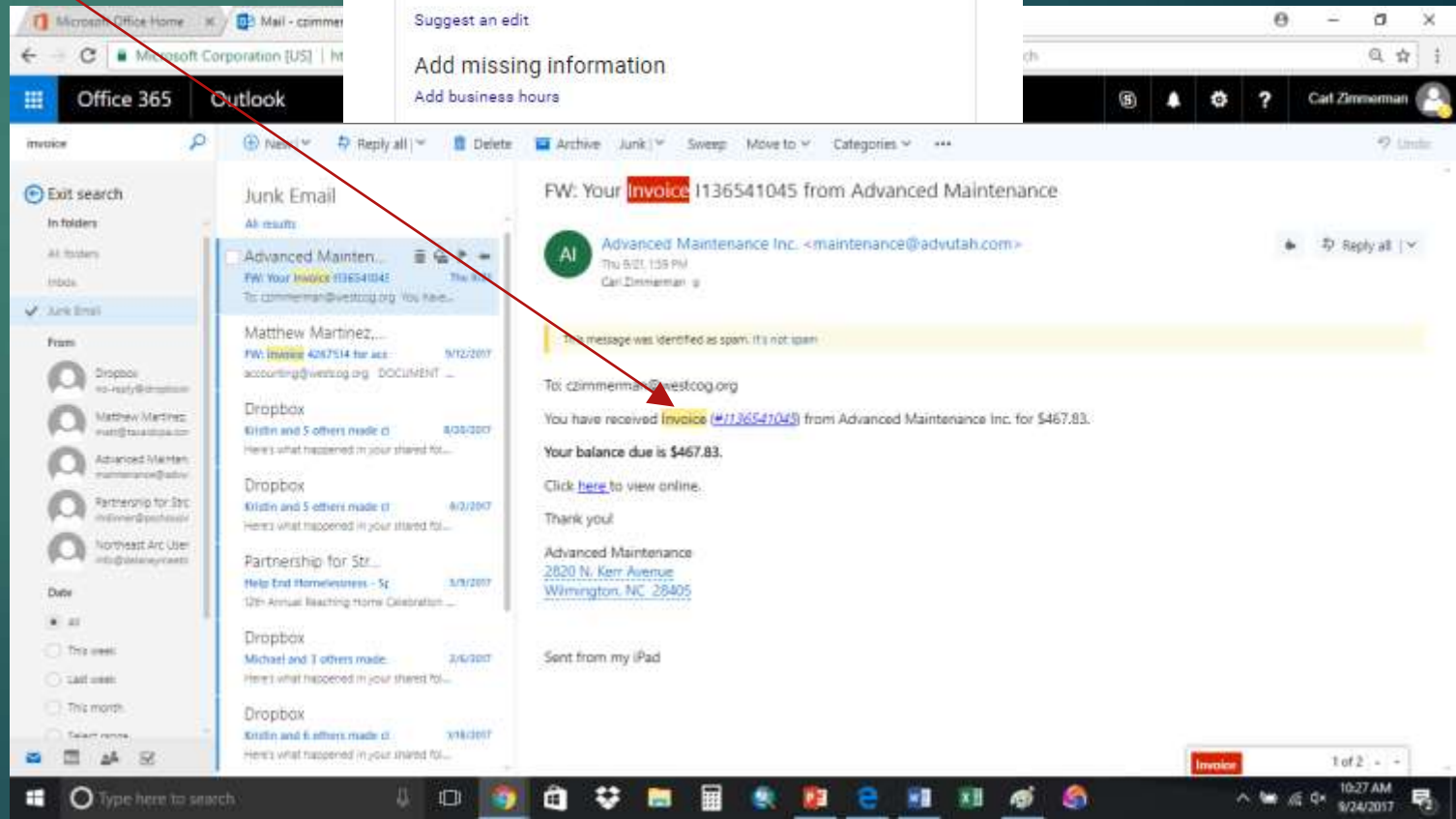


Types of Vulnerabilities

- Malware (watch out for the USB)
- Ransomware (WannaCry)
- Phishing
  - Emails and website intended to steal data or add malware
- Denial of Service
- Social engineering
- Zero-day exploits







Data Vulnerability

- Equifax

Business

Equifax manages 1,200 times more data than the Library of Congress. That's why people are so worried.

Secure | https://www.theverge.com/2017/9/22/16345580/equifax-data-breach-credit-identity-theft-updates

THE VERGE TWEET SHARE

143 million compromised Social Security numbers: everything you need to know about the Equifax

www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site

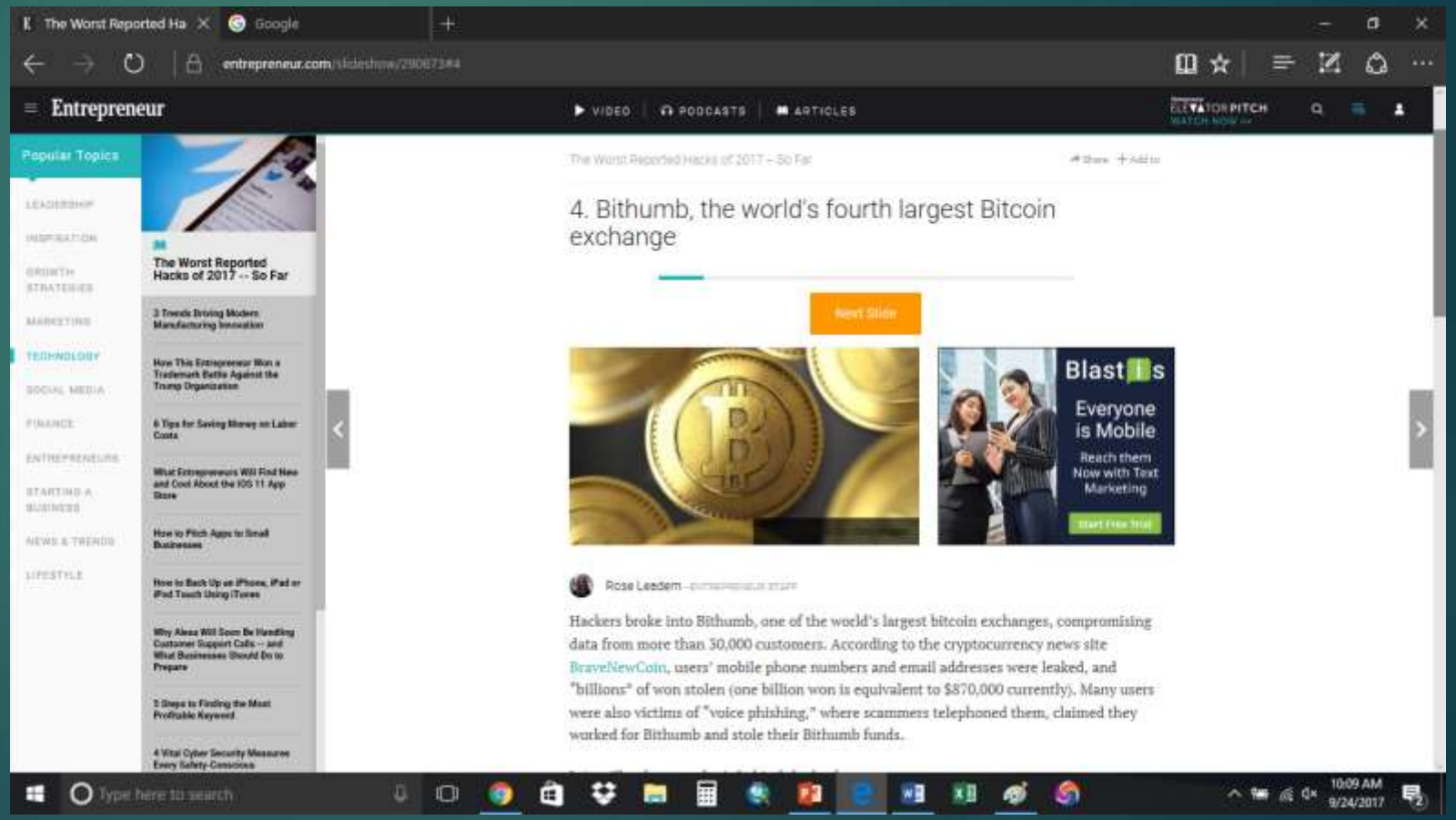
the two-way BREAKING NEWS FROM NPR

MUST READS

After Massive Data Breach, Equifax Directed Customers To Fake Site

Data Vulnerability

- Bithumb



Data Vulnerability/Ransomware

- Wanna Cry
  - Hospitals
  - Manufacturing like Honda

Cyber warfare is Cheap!

- $3.5 billion per Destroyer
  - $10/ 1 million emails
- $76.8 million per F35a
  - $1200/month for DOS type attach
  - Source: FEMA/Teex: Essentials of Community Cybersecurity Training

Is anyone in the board room listening? Photograph by Alexander Zemlianichenko Jr. – Bloomberg/Getty Images

CYBER SECURITY

Why cyber warfare is so attractive to small nations

Cyber Incidents and Attacks

- Events that threaten the confidentiality, integrity and availability of a system or community
- Incident and attack are not synonymous
- Can by caused by attack, glitch, or disasters

- **Confidentiality:** Preserving authorized restrictions
- **Integrity:** Maintaining format and avoid modification
- **Availability:** Timely and reliable access

Characteristics of Cyber Incidents

- **Pre-attack**
  - Data collection and recon and early warning
  - Can ping to find out about the defenses or observe/dumpster dive/open procurement
- **Attack phase**
  - Threats: Single, multiple, persistent
  - Advance Persistent threat
    - Gains access and utilize for long period of time
    - In place or waiting for particular situation (logic bottom)
- **Post attack**
  - Establish back door and destruction of evidence
  - Everything is logged

Types or Impact

- Key: May cause CASCADING IMPACTS
  - Flight cancelation
- Data Breach
  - Heavily regulated industries have higher cost per breach (medical)
- Other Impacts
  - Loss of productivity
  - Trust
  - Market Share
  - Community impacts (loss of critical infrastructure)

Unique Issues in Cybersecurity Planning

- Unique issues:
  - May not have geographic constraints (unlike emergency management) and source can be untraceable
  - Speed of cyber incident is much higher
  - No need to have human interaction (ex. Worms)
  - Often pick open platforms (windows and androids) and exploit open societies
  - Planning team needs to include IT professionals

Definition of Cybersecurity

- The prevention of damage, unauthorized access, exploitation, and restoration if needed of information and communication systems to ensure **three** key factors.
  - Confidentiality
  - Integrity
  - Availability

CIA Triad

- Confidentiality- maintain privacy and limits access
- Integrity - assurance and trust in the system that the data is accurate
- Availability- guarantee of access

confidentiality, integrity, and availability (CIA triad)

Confidentiality, integrity and availability, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

Presidential Directive 8

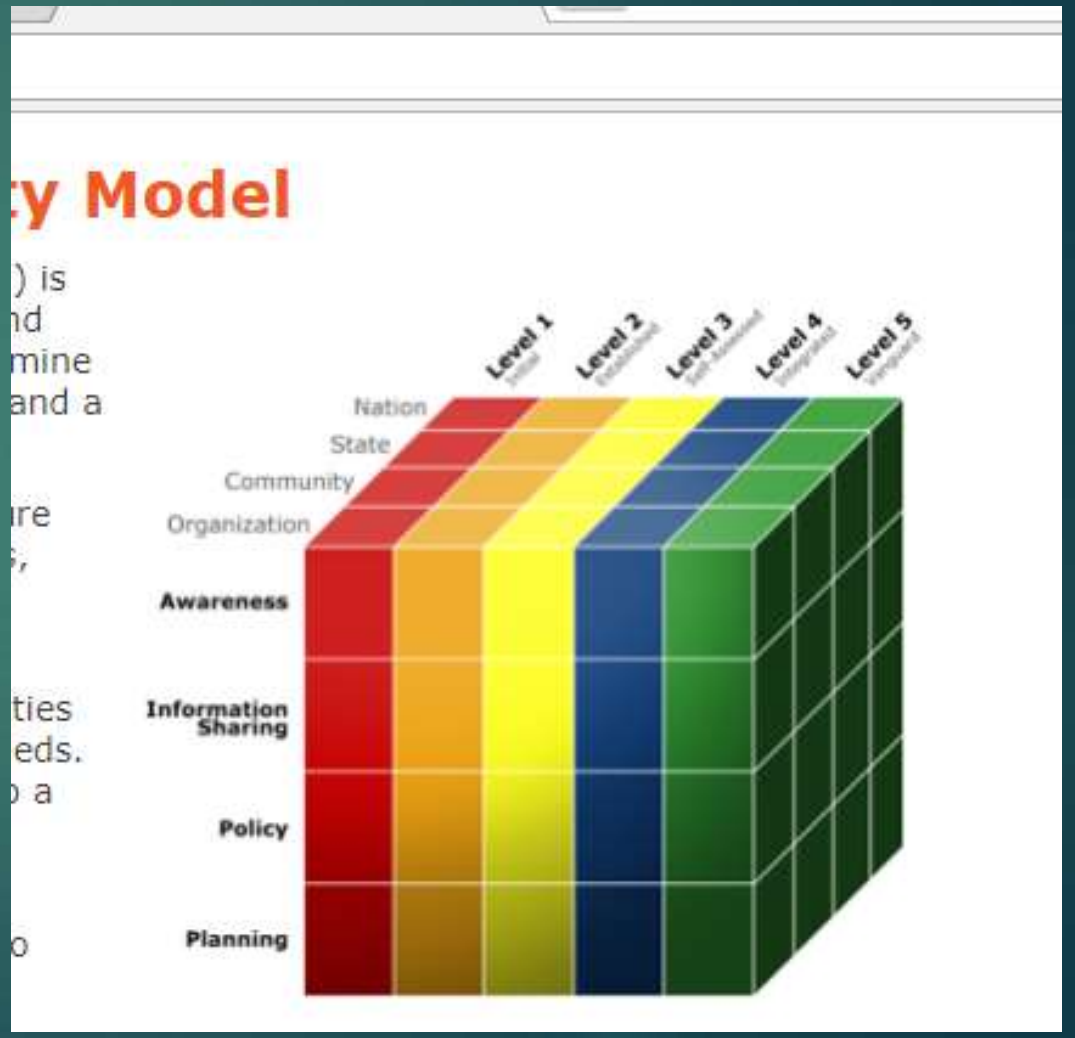
- Obama (2011) and Trump (2017) support
- Directive: Shared responsibility of all levels of government
- Now a primary threat to US security and resilience

Community Cybersecurity

- An entire community and dependencies related to networks
  - Anything connected OR contains networks
  - Critical infrastructure such as hospitals/pharmacies /skada systems
- Ex. Large municipality
  - Tax assessment
  - Traffic infrastructure
  - Police/Fire/Ambulance
  - Fleet Maintenance
  - Computer systems
    - External vendors and apis

Community Cyber Security Maturity Model (CCSMM)

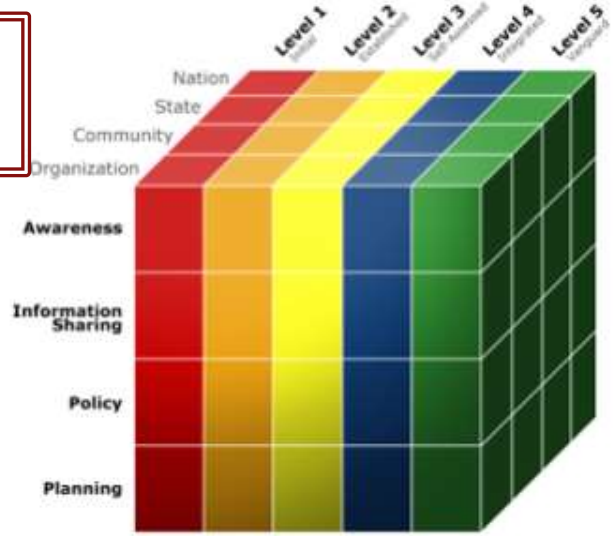
- 5 levels
  - Initial to Vanguard
- Improvement activities
  - Awareness
  - Information sharing
  - Policies and procedures
  - Planning
- Transitioning activities
  - Metrics (benchmarks and baseline)
  - Information sharing
  - Technology
  - Processes, Planning, and Testing



The Community Cyber Security Maturity Model

Developed by the CIAS, the Community Cyber Security Maturity Model (CCSMM) is designed to address the needs of states and communities to develop a viable and sustainable cyber security program. The CCSMM provides a "yardstick" to determine the current cyber security posture, a "road map" to help improve that posture, and a common point of reference to share experiences and lessons learned.

The model identifies the characteristics of communities and states as they mature their cyber security programs. It uses aspects such as cyber security awareness, security policies and procedures, information sharing within and between organizations, and cyber security training and education.



It is not lost on the CIAS that states are made up of communities and communities are composed of organizations and the model addresses these very different needs. It is often depicted in three dimensions to show how its tenets can be applied to a large swath of administrative units.

There are five levels in the CCSMM and organizations, communities and states progress through each of the five levels in order. The transition from one level to another is referred to as a phase and thus there are four phases in the model.

Level 1 - Initial

Organizations, communities and states at this level have little to no cyber security awareness, analysis and assessments. little inclusion of cyber threats and issues in the continuity of operations plans.

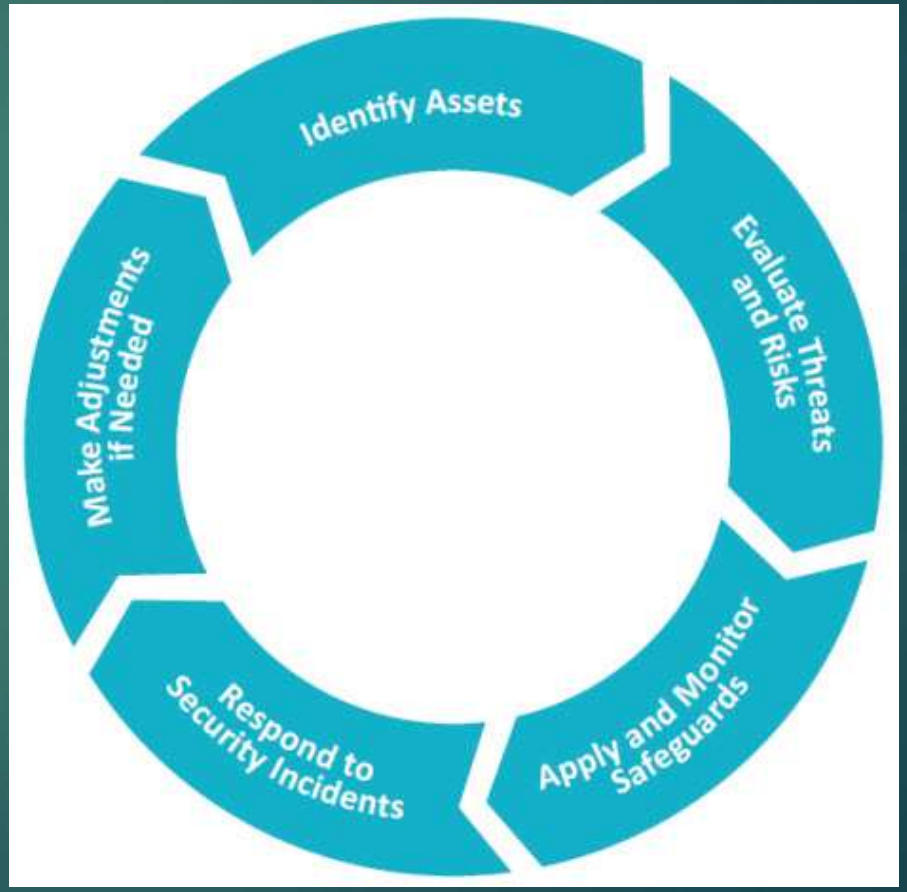
Level 2 - Established

The leadership of organizations, communities and states at this level is aware of cyber threats, issues and the imperative

LEVEL 1 Initial	LEVEL 2 Advanced	LEVEL 3 Self-Assessed	LEVEL 4 Integrated	LEVEL 5 Vanguard
• Minimal cyber awareness	• Leadership aware of cyber threats, issues and imperatives for cyber security and community cooperative cyber training	• Leaders promote org security awareness; formal community cooperative training	• Leaders and orgs promote awareness; citizens aware of cyber security issues	• Awareness a business imperative
• Minimal cyber info sharing	• Informal info sharing/ communication in community; working groups established; ad-hoc analysis, little fusion or metrics; professional orgs established or engaged	• Formal local info sharing/cyber analysis. initial cyber-physical fusion; informal external info sharing/ cyber analysis and metrics gathering	• Formal info sharing/ analysis, internal and external to community; formal local fusion and metrics, initial external efforts	• Fully integrated fusion /analysis center, combining all-source physical and cyber info; create and disseminate near real world picture
• Minimal cyber assessments and policy & procedure evaluations	• No assessments, but aware of requirement; initial evaluation of policies & procedures	• Autonomous tabletop cyber exercises with assessments of info sharing, policies & procedures, and fusion; routine audit program; mentor externals on policies & procedures, auditing and training	• Autonomous cyber exercises with assessments of formal info sharing/local fusion; exercises involve live play/metrics assessments	• Accomplish full-scale blended exercises and assess complete fusion capability; involve/ mentor other communities/entities
• Little inclusion of cyber into Continuity of Operations Plan (COOP)	• Aware of need to integrate cyber security into COOP	• Include cyber in COOP; formal cyber incident response/recovery	• Integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery	• Continue to integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery

Possible Goals and Regional Response

- Regional response could include a Regional or DEMHS oriented work group and task force



How to Start the Planning Process

- **Identify a champion**
  - Vision and enthusiasm
  - Identify and recruit
  - Solicit support and resources
  - Focused and community oriented
  - Communicator

How to Start the Planning Process

- **Cyber preparedness working group**
  - Provide leadership
  - Initiate goals and objective
  - Recruit talent
  - State has a working group?
  - Need credibility, IT aware, and knowledge of community
- Other members
  - Law enforcement
  - Municipal IT
  - School
  - Conndot
  - Private it
  - State rep
  - Hospitals
  - Dehms
  - Education
  - Big Corp
  - Volunteer community
  - Universities

How to Start the Planning Process

- **Determine Goals and Objectives for the Program**
  - Focused, achievable, applicable
  - Need action plan
  - What does success look like (good for plan and interview)

- **For our Region, identify low hanging fruit**

How to Start the Planning Process

- **Develop task force**
  - Diverse collaborative team
  - Specific goals and objectives
  - Awareness
  - Tool chest/ resources
  - Communicate
  - Finally:
    - Implement and evaluate using metric and baseline knowledge

- Summary: Advocating for a regional process regarding Cybersecurity to identify and improve baseline skills and skill/knowledge gaps

Resources for Resiliency

- TEEX training
- Strategic Foresight Initiative
- Stop.Think.Connect
- Federal Communications Cyber Planner
- Center for Internet Security

Questions????

- See our available resources and contact TEEX.org for more information. See some of the following references for more information:
- http://cias.utsa.edu/resources.html
- https://www.us-cert.gov/ccubedvp/cybersecurity-framework
- https://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide_1.pdf
- http://portal.ct.gov/connecticut-cybersecurity-resource-page