FirstNet Applications Workshop

Cybersecurity and Public Safety Networks

Daniel J. Ragsdale, Ph.D.

Director, Texas A&M Cybersecurity Center

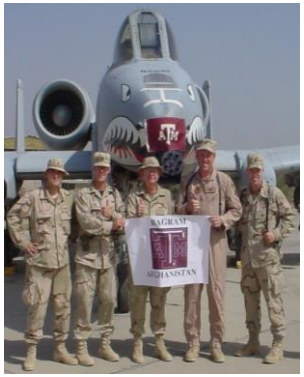
TEXAS A&M UNIVERSITY

BLUF

- **The Threats are increasing and ever-evolving…**
- **…but there is cause for hope!**

My Background

- **Aggie ‘80**
  - **Fish Drill Team, Student Senate**
  - **Ph.D., Computer Science, 2001**
- **37+ Years in Federal Service**
  - **3 Combat Deployments**
- **Cybersecurity Expertise**
  - **Led the establishment of West Point’s World-Class Cybersecurity Program**
  - **4 years at DARPA**
- **Contacts throughout Higher Education, NSF, DoD, DHS, NSA, DARPA, etc.**



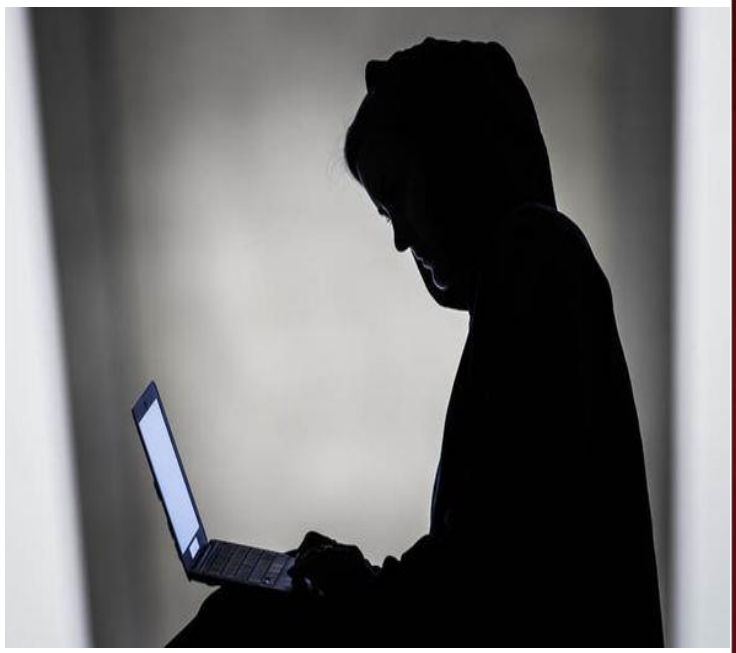
What We're Hearing…

- We're constantly losing ground
- We've already been compromised
- ALL of the IP is gone
- Privacy is dead
- Technology has failed us

What We're Reading…

Cyber hackers are GREATER threat to UK security than nuclear weapons ~ Express 10/25/16

> "We are at greater risk … because we are allowing it to develop without the same international monitoring and management …that we have applied for nuclear weapons."



http://fortune.com/2016/05/18/linkedin-data-breach-email-password/

The (former) Candidates Weigh-in

Cyber-attacks from foreign governments, especially China, Russia, and North Korea along with non-state terrorist actors and organized criminal groups, **constitute one of our most critical national security concerns**. ~ President Elect Donald Trump (Oct 3, 2016)

"**We must hold to account those who are stealing our nation's intellectual capital**….Efforts to expose, prosecute, and in some cases retaliate against these actors will raise the cost of conducting such attacks and increase deterrence of future attacks." ~ Jeb Bush (Strengthening Cybersecurity, 14 Sep 2015)

What We're Reading…

How America's 911 emergency response system can be hacked ~ Washington Post, 9/9/16

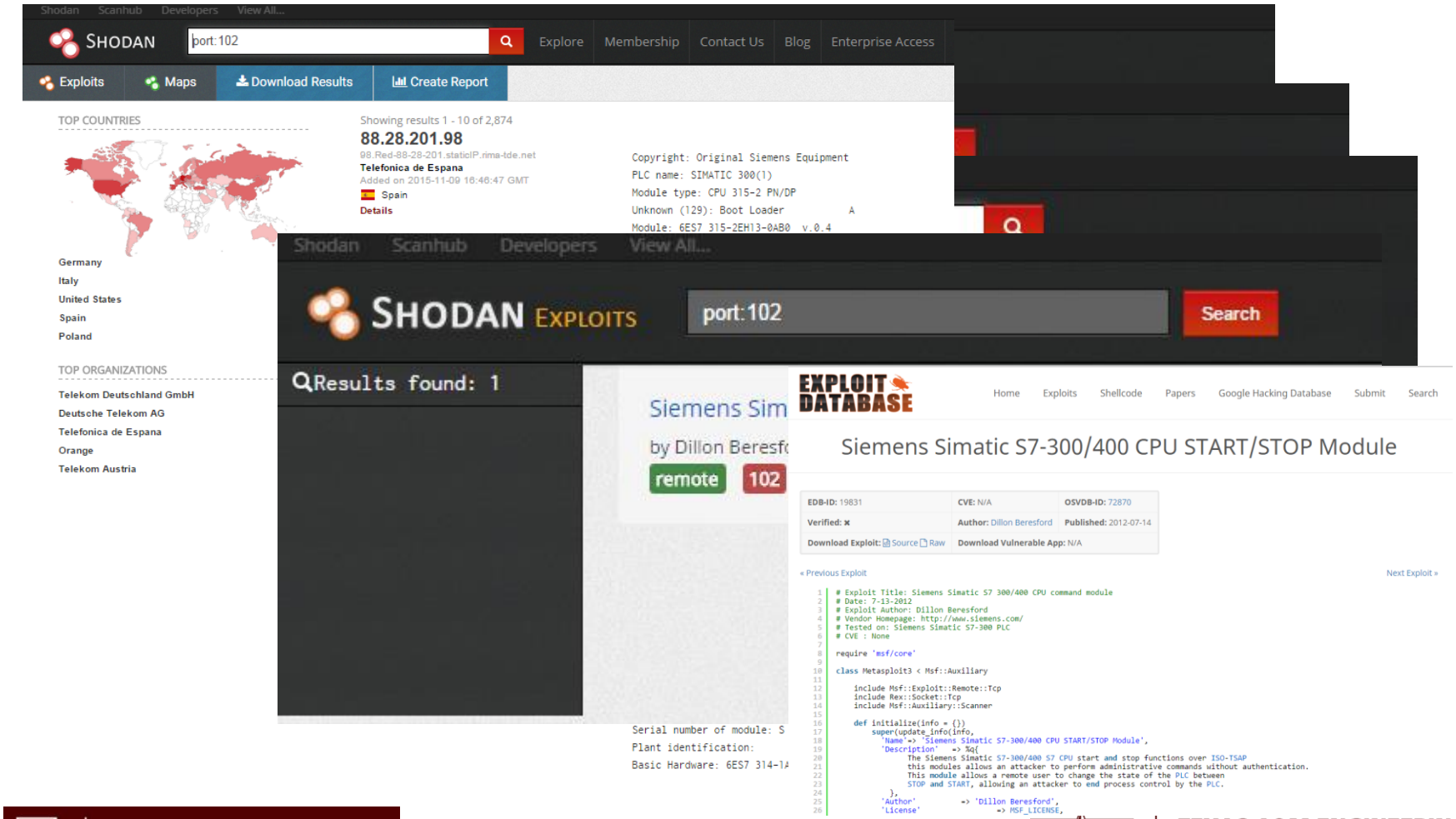
- "…effectively disable the 911 emergency system across an entire state for an extended period of time"
- A "TDoS" attack against call centers involving [a botnet of infected] phones causing them to automatically make bogus 911 calls
- The Israeli researchers built a simulated cellular network based on the 911 network in North Carolina.

What We're Reading…

Arizona Teen Arrested For Disrupting iPhone 911 Emergency Service~ E Hacking News Post, 10/31/16

- He "created a JavaScript exploit, which he shared with his friends on Twitter and other websites…"
- "Users who clicked on it had their iPhones automatically and repeatedly dial 911. "
- "The volume of the calls allegedly put the responders and authorities 'in immediate danger of losing services to their switches' "

Shodan: Discover the Internet…



What We're Reading…

Massive Friend Finder Network Breach ~ Tech Target 11/15/16

Of the more than 400 million Friend Finder Network (FFN) user accounts exposed,

-125.6 million had passwords stored in plain text and

- 282 million passwords stored using the obsolete SHA-1 algorithm

http://fortune.com/2016/05/18/linkedin-data-breach-email-password/

The 25 Most Popular Passwords:

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

We're All Doomed!

http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

What We're Reading…

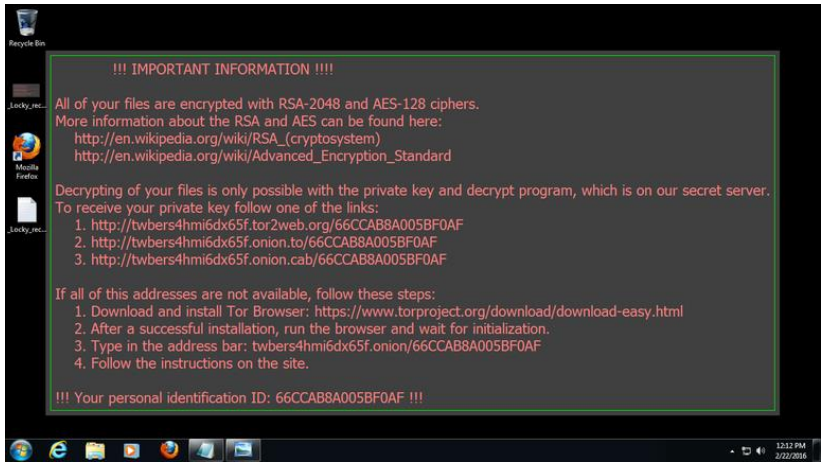
Crypto-ransomware Attacks Rise 5-fold to Hit 718K Users in One Year ~ Kaspersky Lab, June 23, 2016

"…one of the most dangerous types of malware ever created"

This ransomware is now one of the three most common malware threats

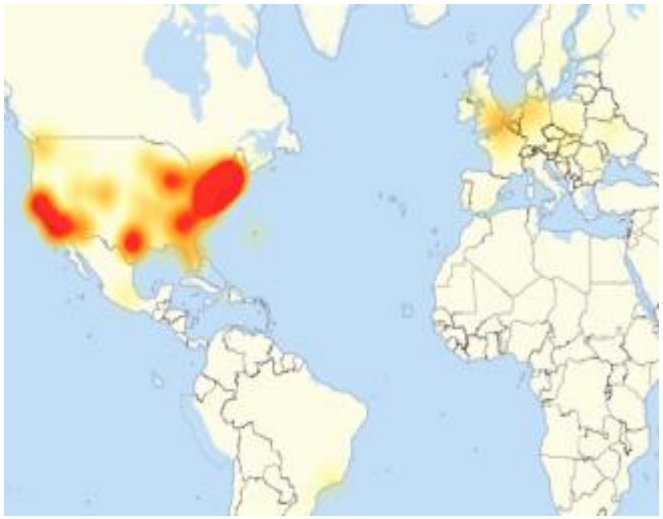
~ZDNet 10/20/16

"The total cost of damages related to these attacks is set to top $1 billion this year"



What We're Reading…

How your DVR was hijacked to help epic cyberattack ~ USA Today 10/23/16



I am GUESSING that Twitter's DNS is under attack

The massive siege on Dyn caused outages on Amazon, Twitter, Netflix, Etsy

Mirai botnet built "using malware from phishing emails to first infect a computer, then spreads to everything [it can connect to], taking over DVRs, cable set-top boxes, routers and even Internet-connected cameras"

What We're Reading…

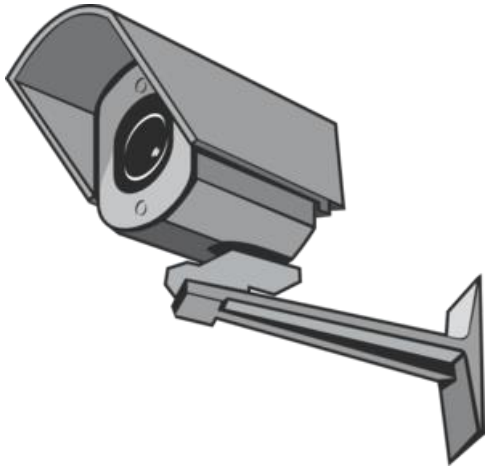
5 Russian Banks Hit By IoT DDoS Attack ~ Dark Reading, 11/11/16

"…attackers used a variety of Internet of Things devices like DVRs and webcams to launch the DDoSes…"

" …24,000 hijacked devices located in 30 countries"

Russian banks floored by withering DDoS attacks ~ The Register 11/11/15

"If the default [manufacturer's] password had been changed, many of the webcams and CCTV devices that formed the botnet army would not have been successfully hijacked."



What We're Reading…

The Big Lesson We Must Learn From The Dyn DDoS Attack ~ Dark Reading 11/9/16

"The vulnerabilities that make IoT devices susceptible to being used in a botnet also make them the perfect avenue into our data centers and clouds"

"But systemic IoT security flaws leave us vulnerable to many kinds of attacks. DDoS may be the least of our worries."

What we are Reading..

LastPass, Defender of Our Passwords, Just Got Hacked
~ GIZMODO, June 16, 2016

- "No evidence that encrypted user vault data was taken, nor that LastPass user accounts were accessed…"
- Enable two-factor authentication

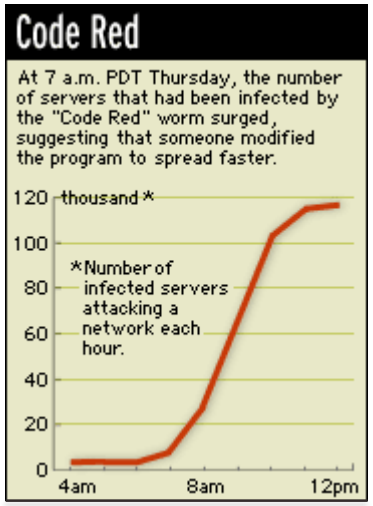
https://ytimg.googleusercontent.com/vi/_du1R45ErJo/hqdefault.jpg

Most Common Used Vectors to Gain Access

- **Spear Phishing**
  - Email that appears to be from someone you know
  - Often highly personalized
- **Watering Hole Attacks**
  - Attacker guesses or observes websites a group use often uses and infects one or more of them with malware
- **Less common: Pharming, XSS, SQL Injection, CXRF**

What we are Seeing…..

- Code Red Worm (2001)
  - Visualization
- Ongoing Attacks (2016)
  - Norse Attack Map



Time Check…

Why are we seeing this?

- “Arms Race”
- Complexity++
- Interconnectivity++
- Market Forces
- “Unholy Alliances”
- Educational Practices

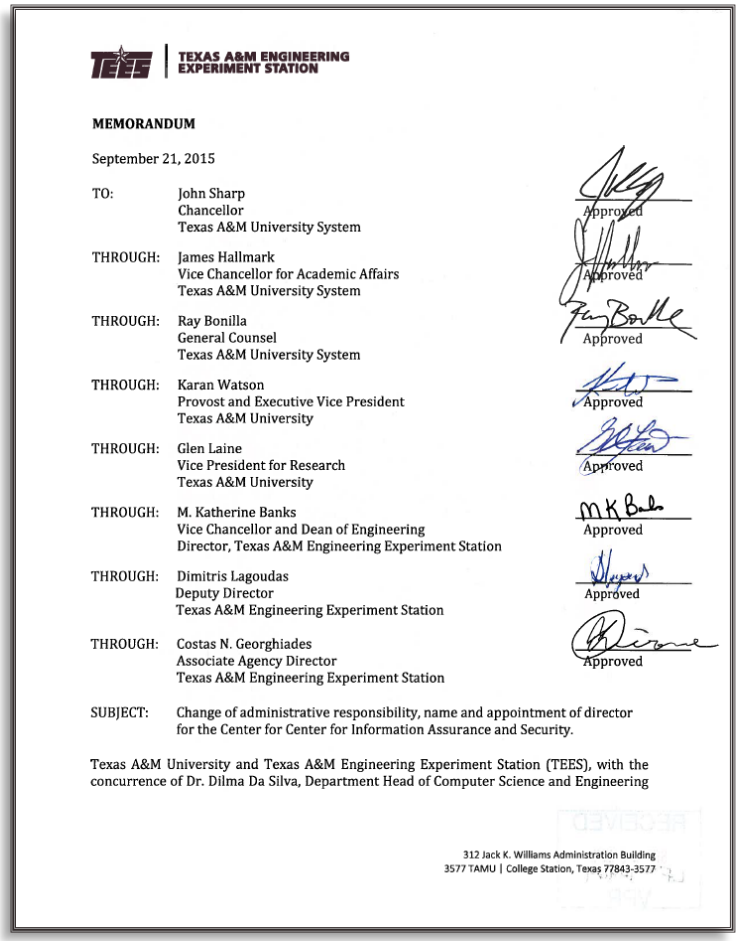
http://www.kesolutions.biz/News-Entry-srk/Internet-of-things--what-does-it-have-to-do-with-my-small-business--bek /

https://www.reportingproject.net/unholyalliances/img/project-logo.jpg

So…

TAMC2

The Texas A&M Cybersecurity Center



TEES | TEXAS A&M ENGINEERING EXPERIMENT STATION

MEMORANDUM

September 21, 2015

TO: John Sharp
Chancellor
Texas A&M University System
Approved

THROUGH: James Hallmark
Vice Chancellor for Academic Affairs
Texas A&M University System
Approved

THROUGH: Ray Bonilla
General Counsel
Texas A&M University System
Approved

THROUGH: Karan Watson
Provost and Executive Vice President
Texas A&M University
Approved

THROUGH: Glen Laine
Vice President for Research
Texas A&M University
Approved

THROUGH: M. Katherine Banks
Vice Chancellor and Dean of Engineering
Director, Texas A&M Engineering Experiment Station
Approved

THROUGH: Dimitris Lagoudas
Deputy Director
Texas A&M Engineering Experiment Station
Approved

THROUGH: Costas N. Georghiades
Associate Agency Director
Texas A&M Engineering Experiment Station
Approved

SUBJECT: Change of administrative responsibility, name and appointment of director for the Center for Center for Information Assurance and Security.

Texas A&M University and Texas A&M Engineering Experiment Station (TEES), with the concurrence of Dr. Dilma Da Silva, Department Head of Computer Science and Engineering

312 Jack K. Williams Administration Building
3577 TAMU | College Station, Texas 77843-3577

The formation of a "new" Joint TEES and Texas A&M Center

http://cybersecurity.tamu.edu/

TEXAS A&M CYBERSECURITY CENTER

TEES | TEXAS A&M ENGINEERING EXPERIMENT STATION

Vision

The Texas A&M System will make outsized contributions to national and economic security and social good by advancing the knowledge and the practice of cybersecurity, and by developing transformational cybersecurity capabilities.

The Texas A&M System, in collaboration with strategic partners, will move to the international forefront of cybersecurity research, education, and training.

Mission

- **Facilitate the conduct of ground-breaking, basic and applied cybersecurity research**
- **Develop novel and innovative methods for cybersecurity education, training, and workforce development**
- **Build mutually beneficial and fruitful partnerships with commercial, governmental, military, and academic partners**

The Feds

Recent Legislation: Cybersecurity Information Sharing Act of 2015

- Federal agencies must develop procedures to share cybersecurity threat information with
  - Private entities, nonfederal government agencies, the public, and entities under threats
- Provides liability protections
- DHS will develop processes to:
  - Receive indicators and defensive measures that are shared by any entity
  - Ensure that appropriate federal entities receive shared indicators in an automated, real-time manner.

National Directives

- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013)**
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

National Directives (cont.)

- **Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013)**
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

National Directives (cont.)

- **Promoting Private Sector Cybersecurity Information Sharing (2013)**
  - An Executive Order to create [broader] Information Sharing and Analysis Organization program (ISAOs)
  - ISAOs may be organized on the basis of:
    - sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities
  - Note: The Emergency Management & Response ISAC (EMR-ISAC) is administered by FEMA and the U.S. Fire Administration
    - Information Sharing Groups

DHS ESS Resources

- **Emergency Services Sector-Cyber Risk Assessment (ESS-CRA)**
  - An initial [2012] sector-wide assessment that analyzed strategic cyber risks to ESS infrastructure
- **Cyber Resilience Review**
  - A no-cost, voluntary program to evaluate and enhance cybersecurity capacities and capabilities within all 16 critical infrastructure sectors
- **Emergency Services Sector Roadmap to Secure Voice and Data Systems**
  - Identified and discussed proposed risk mitigation measures to address risks identified in the ESS-CRA

DHS ESS Resources (cont.)

- **Enhanced Cybersecurity Services**
  - A voluntary information-sharing program to improve protection of ESS systems from unauthorized access, exploitation, or data exfiltration.
- **Emergency Services Sector Cybersecurity Framework Implementation Guidance**
  - Enhance the ability of member of the Emergency Services Sector to:
    - Better understand and manage cyber risks
    - Coordinate sharing of cyber information and cyber capabilities

DHS Cyber Resilience Review (CRR)

- Asset Management
  - Processes used to identify, document, and manage the organization's assets.
- Controls Management
  - Processes used to define, analyze, assess, and manage the organization's controls.
- Configuration and Change Management
  - Processes used to ensure the integrity of an organization's assets.
- Vulnerability Management
  - Processes used to identify, analyze, and manage vulnerabilities within the organization's operating environment.
- Incident Management
  - Processes used to identify and analyze events, declare incidents, determine a response and improve an organization's incident management capability.
- Service Continuity Management
  - Processes used to ensure the continuity of an organization's essential services.
- Risk Management
  - Processes used to identify, analyze, and manage risks to an organization's critical services.
- External Dependencies Management
  - Processes used to establish an appropriate level of controls to manage the risks that are related to the critical service's dependence on the actions of external entities.
- Training and Awareness
  - Processes used to develop skills and promote awareness for people with roles that support the critical service.
- Situational Awareness
  - Processes used to discover and analyze information related to the immediate operational stability of the organization's critical services and to coordinate such information across the enterprise

https://www.dhs.gov/sites/default/files/publications/Cyber-Resilience-Review-Fact-Sheet-508.pdf

ESS Roadmap to Secure Voice and Data Systems (2014)

Cyber Risk Mitigation Measure	Federal Influence or Engagement
Adopt and Implement Next Generation 9-1-1 Services	Heavy
Create and Implement an Alternative Emergency Number to 9-1-1 and/or Expand the Number of Available 9-1-1 Trunk Lines	Little or none
Create Alternate Emergency Operation Centers and Additional Public Safety Answering Point Facilities	Little or none
Create Diversity in Public Safety Answering Point and Communications Infrastructure Facilities	Little or none
Implement Improved Physical Security Measures at Public Safety Answering Point and Communications Infrastructure Facilities	Little or none
Adopt and Implement Rollover Capabilities in Public Safety Answering Point and Emergency Operation Center facilities	Little or none
Conduct and Evaluate Failover Capabilities through Exercises	Little or none
Establish Comprehensive Cybersecurity and Continuity of Operations Plan Implementation Training and Education for Staff	Moderate
Create Hot Continuity of Operations Sites with Database Backups	Little or none
Evaluate the Use of Amateur Radio Networks, Talk-Around Channels, and Talk Groups and Establishing an Area Command to Manage Consequences of Incidents	Little or none
Implement Public Alerting and Warning Systems to Provide Guidance for the Public	Little or none
Adopt and Implement Security Policies and Procedures to Protect Sector Databases and Public Alerting and Warning Systems	Little or none
Implement Standards, Guidelines, and Best Practices for Surveillance Technologies and Capabilities	Little or none
Evaluate the Physical Location of Cameras and Other Surveillance Technologies	Little or none
Implement Artificial Intelligence to Assist with Monitoring and Tracking Potential Risks	Little or none

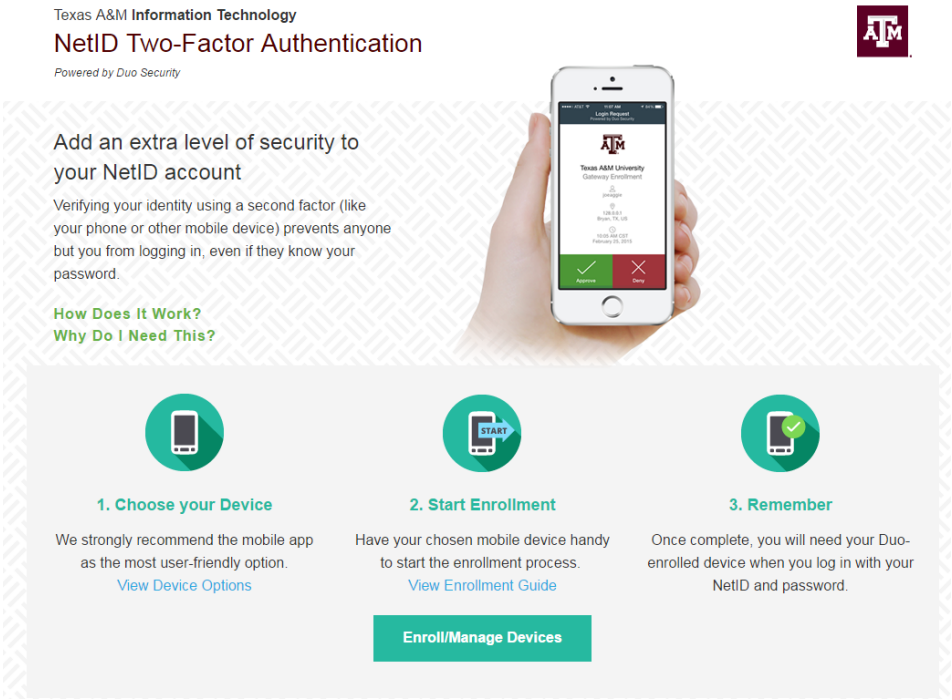
DHS Emergency Services Sector Information Sharing Initiative

- **Goal: Increase the use and improve the quantity and quality of FOUO) and LES content**
  - **Through coordination with the FEMA Emergency Management & Response-Information Sharing and Analysis Center (EMR-ISAC) and the Homeland Security Information Network-Emergency Services (HSIN-ES)**
- **Maintain current relationships and develop new relationships with ESS stakeholders for the timely and effective dissemination of information, including:**
  - **Protective Security Advisors (PSA)**
  - **Cybersecurity Advisors (CSA)**
  - **Fusion Centers**
  - **National Infrastructure Coordinating Center (NICC)**
  - **National Cybersecurity and Communications Integration Center (NCCIC)**

Some Recommendations (Mostly General and Tactical)

Use 2-Factor Authentication (2FA)

- A Type of multi-factor authentication
  - Know
  - Have
  - Are
- What do we all have?



Use (or License) Password Managers

- Passwords
  - Change Passwords frequently
  - Don’t share passwords
  - Use “hard to guess,” i.e., hard to remember passwords
  - Use unique passwords for every site
    - Therefore : USE A PASSWORD MANAGER
- Typically installs as a browser plug-in to “handle capture and replay” of passwords
- Often include a built-in “hard password” generator
- Can sync passwords across multileg devices

Other (Tactical) Best Practices

- Use “modern” operating systems
- Keep all software up-to-date (opt-in for automatic updates)
- Frequently backup data
- Never allow personal activities (browsing, email, etc) on official systems
- “Disable” all email links
- Strip all attachments
- No thumb drives!

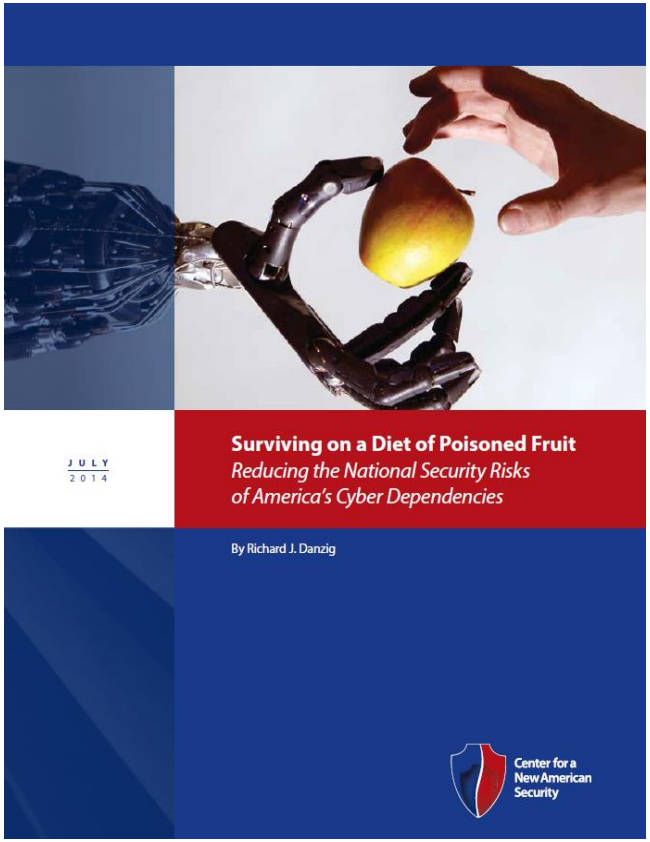
Additional Recommendations

- Conduct exercises with (realistically) degraded systems
- Insist on redundant backup systems
- Isolate/segregate systems wherever possible

Surviving on a Diet of Poisoned Fruit

Report Recommendations

- Articulate a national security standard defining what it is imperative to protect in cyberspace
- **Pursue a strategy that self-consciously sacrifices some cyber benefits in order to ensure greater security for key systems on which security depends**
- Establish a federally funded research and development center focused on providing an elite cyber workforce for the federal government



TEXAS A&M CYBERSECURITY CENTER

TEES | TEXAS A&M ENGINEERING EXPERIMENT STATION

Questions / Discussion