U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Cybersecurity Threats to Critical Infrastructure

Ian Moore, CISSP
Cybersecurity State Coordinator (CSC) for Washington State
Cybersecurity Advisor (CSA) Program
Cybersecurity and Infrastructure Security Agency

Challenge - Rules of Engagement

I've placed molecules throughout this presentation that when grouped together will identify a dangerous compound previously used by many people.

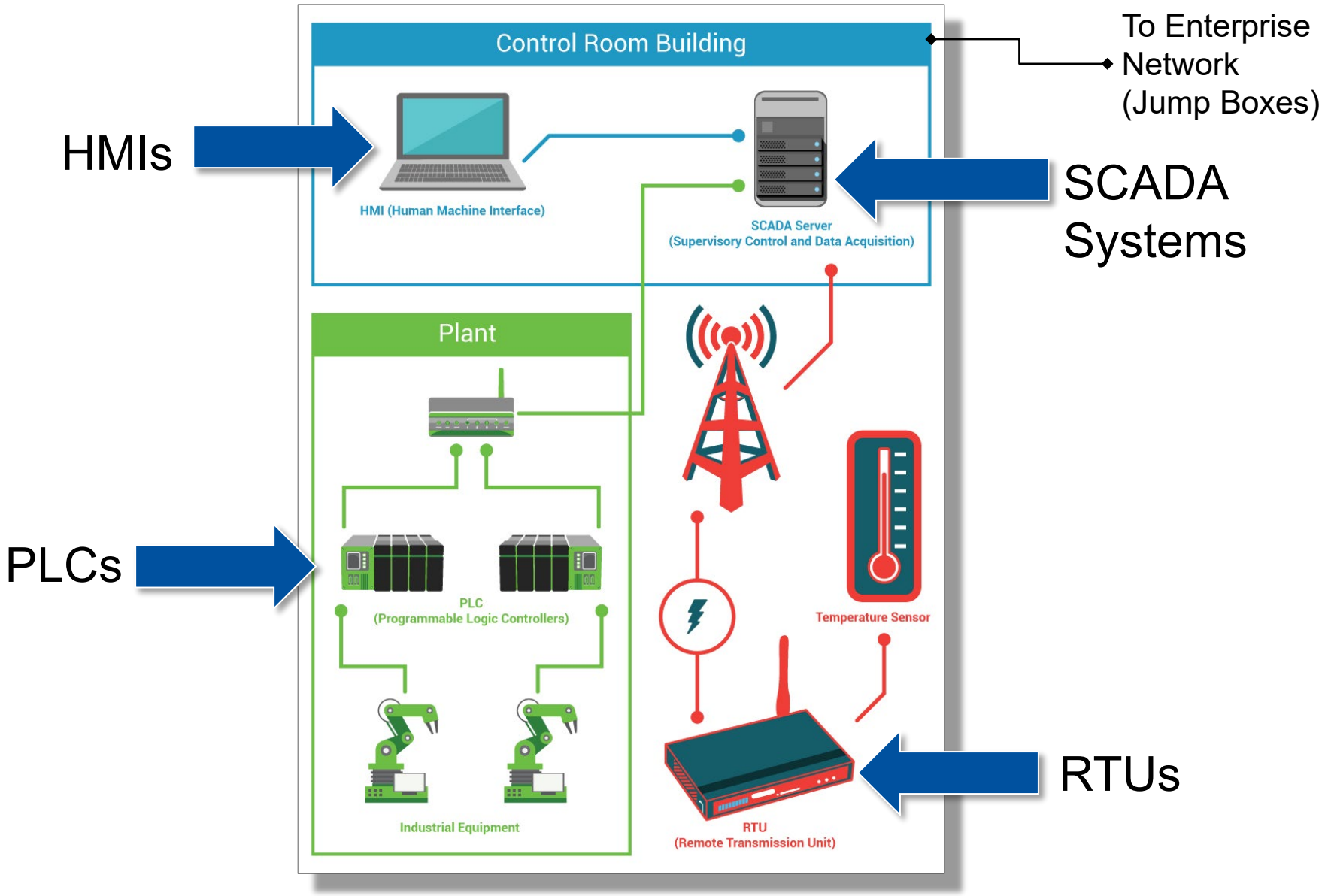
Collect all the molecules, guess the compound (the common name), and write your guess on the back of your business card and bring it to the CISA booth to get a prize. Google is your friend. ;-)

- Only 1 prize per person, the first 20 get a prize

Contents

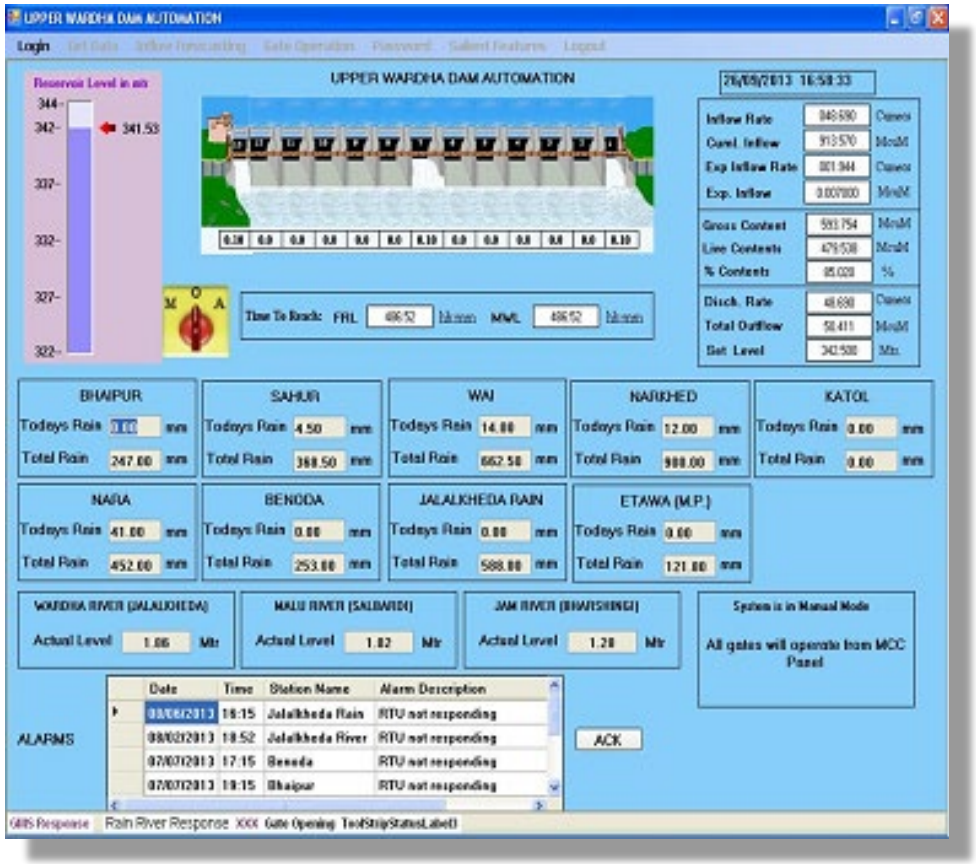
- Supervisory Control and Data Acquisition (SCADA) systems
- Human Machine Interfaces (HMIs)
- Programmable Logic Controllers (PLCs)
- Remote Transmission Units (RTUs)
- Jump Boxes
- Dam Information!
- Ransomware and the OT Environment
- Mitigations
- Take-Aways

Sample Simple Operational Technology Environment



Supervisory Control and Data Acquisition (SCADA) Systems

- A system of software and hardware elements that allows industrial organizations to: Control industrial processes locally or at remote locations. Monitor, gather, and process real-time data.
- Connections to the network and devices
  - wired and wireless
- Unique ports and protocols
- Connects servers, databases, and software



Human Machine Interfaces (HMI)

- The HMI is the operator window of the SCADA system. It presents plant information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the plant being controlled, and alarm and event logging pages.
- Unique ports and protocols
- Manage vendor patching and upgrades
- Proprietary and numerous

Programmable Logic Controllers (PLCs)

- A programmable logic controller (PLC) or programmable controller is an industrial computer that has been ruggedized and adapted for the control of manufacturing processes.
- A device that does only what it is programmed to do
- Software and Programmer limitations
- Developed language vs. program language

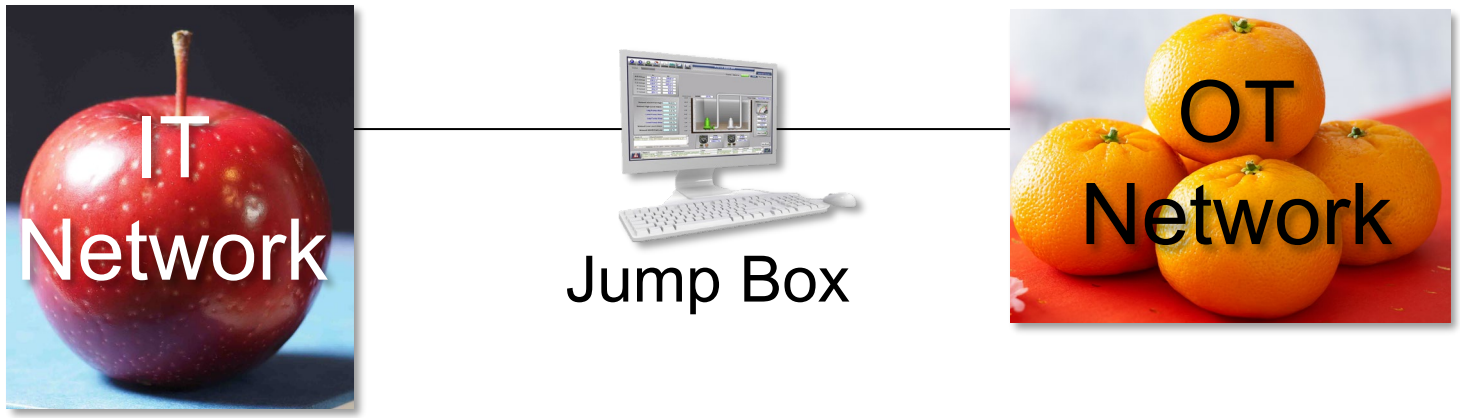
Remote Terminal/Transmission Units (RTUs)

- A remote terminal/transmission unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a SCADA system by transmitting telemetry data to a master system, to control connected objects.
- How they connect (Cellular, RF, or other wireless)
- May not be encrypted
- Potential hardware and software vulnerabilities

Jump Boxes

Hardened and locked-down systems used for connections into OT environments

- Could be old OS and software versions
- May not be a domain-joined computer
  - Vulnerability scanning and being monitored
- Unique ports and protocols
- Could allow multiple connections



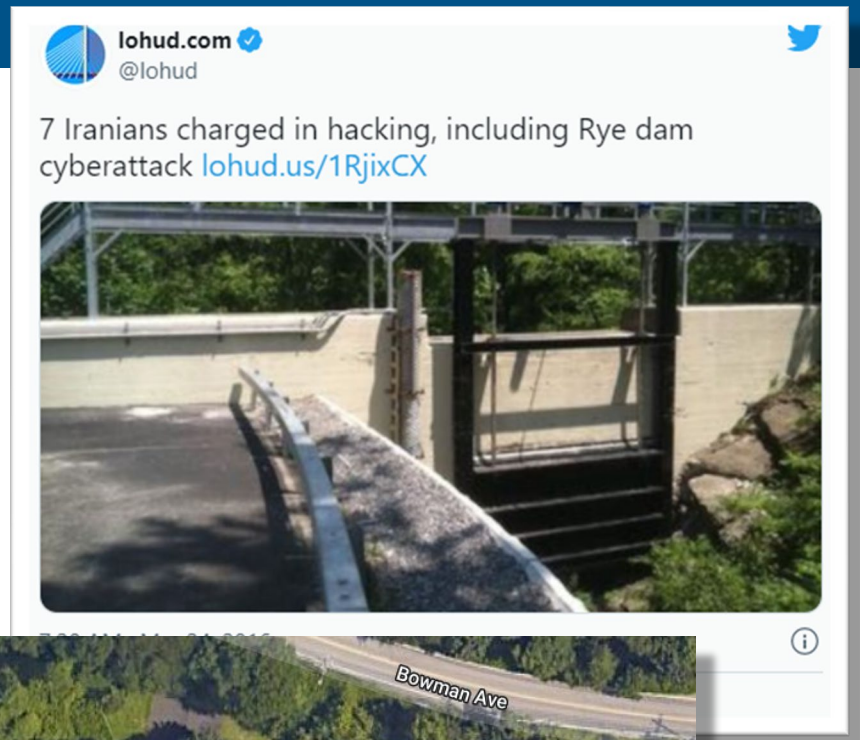
Dam Information!

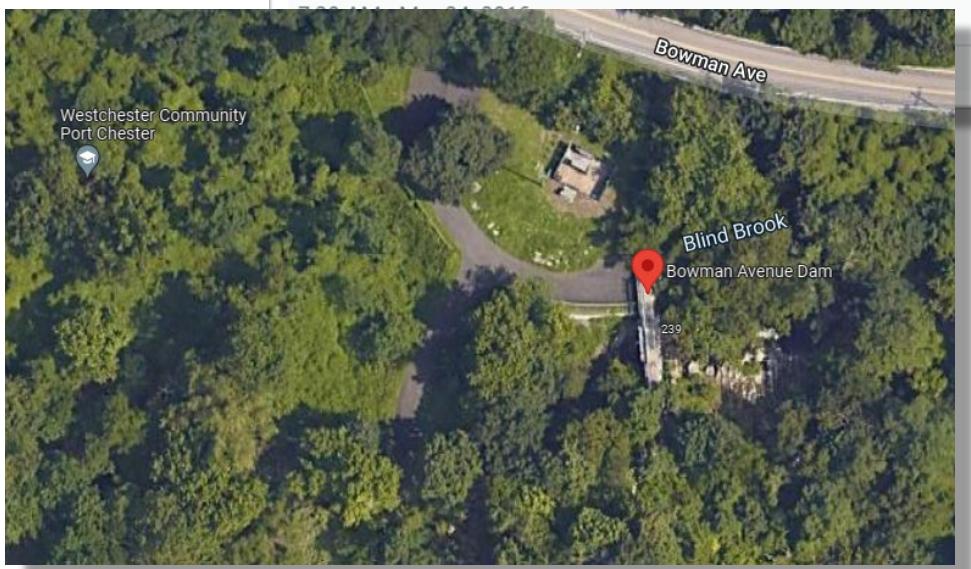
- Recent ICS Vulnerability
  - BadAlloc Vulnerability Affecting BlackBerry QNX Real-time Operating Systems (RTOS)
  - A collection of 25 vulnerabilities

Ask your vendors

- Risks to dams
  - Unknown connections
  - Insider Threat
  - Unmonitored Internet access

- Hacking of the Bowman Avenue Dam in Rye Brook, New York in 2015
  - Allegedly targeted by the Iranians – 7 charged
  - The SCADA system connects to the Internet through cellular modem



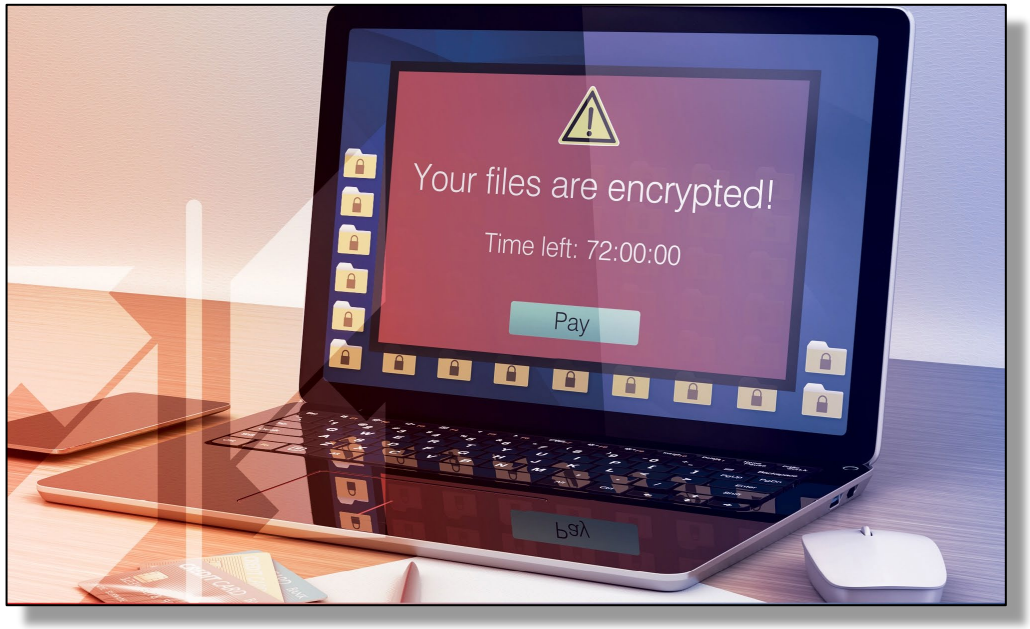


https://www.cisa.gov/publication/dams-cybersecurity-framework-implementation-guidance

Ransomware and the OT Environment

F15

- Ransomware is malware that encrypts your data that the attacker can use for extortion or to demand a ransom.
  - OT Challenges
    - Remote access connections
    - Vendor reliance and access
    - Old and expensive equipment and software
    - Unique ports and protocols
    - Vulnerability scanning difficulty
    - Redundancy and backups may be cost prohibitive
    - May shutdown OT with infected IT
    - Unmonitored Internet access
    - Network not segmented



Mitigations You Can Do Now!

- Network Segmentation
- Multi-factor authentication
- Strong spam filters
- User training program
- Filter network traffic
- Limit access to resources over networks
  - Restrict and secure RDP and SMBv1
- Set antivirus/antimalware programs to conduct regular scans
- Prevent unauthorized execution by:
  - Disabling macro scripts
  - Implementing application allowlisting
  - Monitor and/or block inbound connections
  - Detect and/or ***block*** inbound connection from ***Cobalt Strike*** C&C servers
- Establish and test a robust backup program
  - Frequent backups (full and incremental)
  - 3-2-1 – (Example: 3 copies, 2 different media onsite, and one copy offsite)
  - Test by recovering from backups on a set schedule

Mitigations for CI Owners

- CISA and FBI urge Critical Infrastructure owners and operators to apply the following mitigations:
  - Implement network segmentation between IT and OT networks
  - Use DMZs, logical zones, define acceptable comms between the zones
  - Filter network traffic and monitor communications between zones
  - Prohibit industrial control system (ICS) protocols from traversing the IT network

Take-Aways / Conclusion

- O_2 Understanding Your Vulnerabilities
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Human Machine Interfaces (HMIs)
  - Programmable Logic Controllers (PLCs)
  - Remote Transmission Units (RTUs)
  - Jump Boxes

  } Awareness of their vulnerabilities

- Dam Information!
- Ransomware and the OT Environment
- Mitigations You Can Do Now!
- Mitigations for CI Owners

https://www.cisa.gov/publication/dams-cybersecurity-framework-implementation-guidance

Region 10 Cybersecurity Contacts and Questions?

Chris Callahan
Chief, Cybersecurity (CCS)
(202) 702-6706
CHRISTOPHER.CALLAHAN@cisa.dhs.gov

Theresa Masse
CSC for Oregon
503-930-5671
theresa.masse@cisa.dhs.gov

Josh Stemp
CSC for Idaho
208-761-9882
joshua.stemp@cisa.dhs.gov

Ron Watters, GSLC
Region 10 (WA, OR, ID, AK)
Cybersecurity Advisor
(206) 348-4071
Ronald.Watters@cisa.dhs.gov

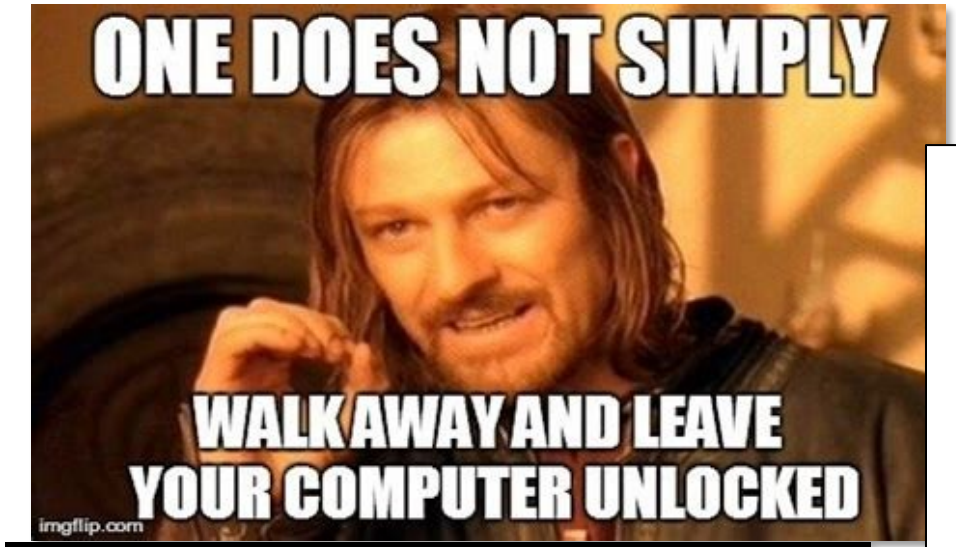
Mark Breunig
CSC for Alaska
907-795-5673
mark.breunig@cisa.dhs.gov

Ian Moore
CSC for Washington
(360) 594-1832
Ian.Moore@cisa.dhs.gov

Contact CISA (via the reporting portal or by phone at 1-888-282-0870) to report an intrusion or to request either technical assistance or additional resources for incident response.
CyberLiaison@cisa.dhs.gov

For inquiries or further information, contact cyberadvisor@cisa.dhs.gov

Meme Break


ONE DOES NOT SIMPLY
WALK AWAY AND LEAVE YOUR COMPUTER UNLOCKED
imgflip.com


PATCH
ALL THE THINGS!
imgflip.com


I SEE CYBER RISKS
EVERYWHERE


Cyber Security
What the government thinks I do
What my friends think I do
What I think I do
What I really do


ILL MAKE THEM DO CYBER AWARENESS TRAINING
AND THEN
ILL MAKE THEM DO IT AGAIN AND AGAIN


IN CASE OF CYBERATTACK
BREAK GLASS AND PULL CABLES


CYBERSECURITY IN A NUTSHELL
KEEP OUT
OR ENTER.
I'M A SIGN, NOT A COP