The Changing Cyber Threat Landscape

Prof. Steve Foster
and
Cybersecurity Project Director
November 2016

WORKFORCE DEVELOPMENT
Thomas Nelson
COMMUNITY COLLEGE

Regional Population and Military Concentration

The Virginia Greater Peninsula is home to **1,699,925** people living in eleven cities/counties

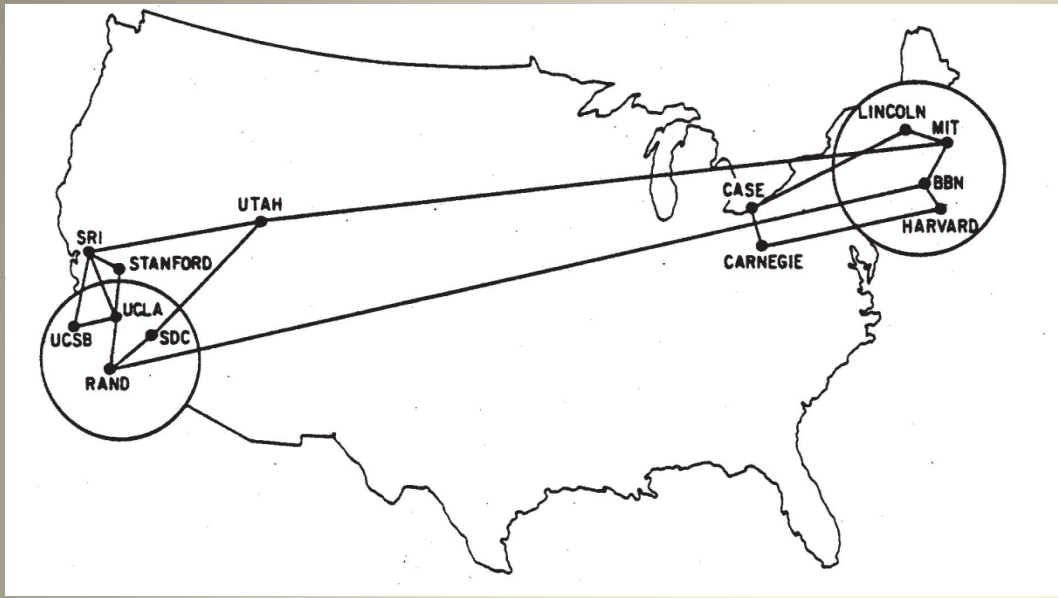
WORKFORCE DEVELOPMENT
Thomas Nelson
COMMUNITY COLLEGE

Did You Know That?

- Today Cybercriminals caused cash to spew from ATM's in Taiwan and Thailand
- There are currently 1 Million Cybersecurity jobs are open Nation wide
- That number goes up to 1.4 M open positions by 2020
- Federal and State Governments are offering free tuition to encourage Cyber Students
- We also expect 50 billion devices connected to the Internet by 2020
- VA Beach a Hub for (2) new undersea transatlantic fiber optic cables from Spain
- VA Gov. in process of making VA Cyber Capital of the USA
- Military has conceded a portion of there own networks to Hackers
- We have no National Cyber Policy or plan to define a Cyberwar and or response
- China wants to compete with CISCO, ha, ha
- Verizon is beginning to offer upstream Cybersecurity options

Do I have your attention yet

Birth of the Internet 1969



IBM 1960's Mainframe computer

DARPA was created in **1958** as the Advanced Research Projects Agency (ARPA) by the Dept. of Defense (DoD) to execute R&D projects and survive a Nuclear attack during the "Cold War".

DARPA's involvement in the **creation of the Internet** began with an idea to link time-sharing computers into a National system.. The **first Node was connected in 1969**.

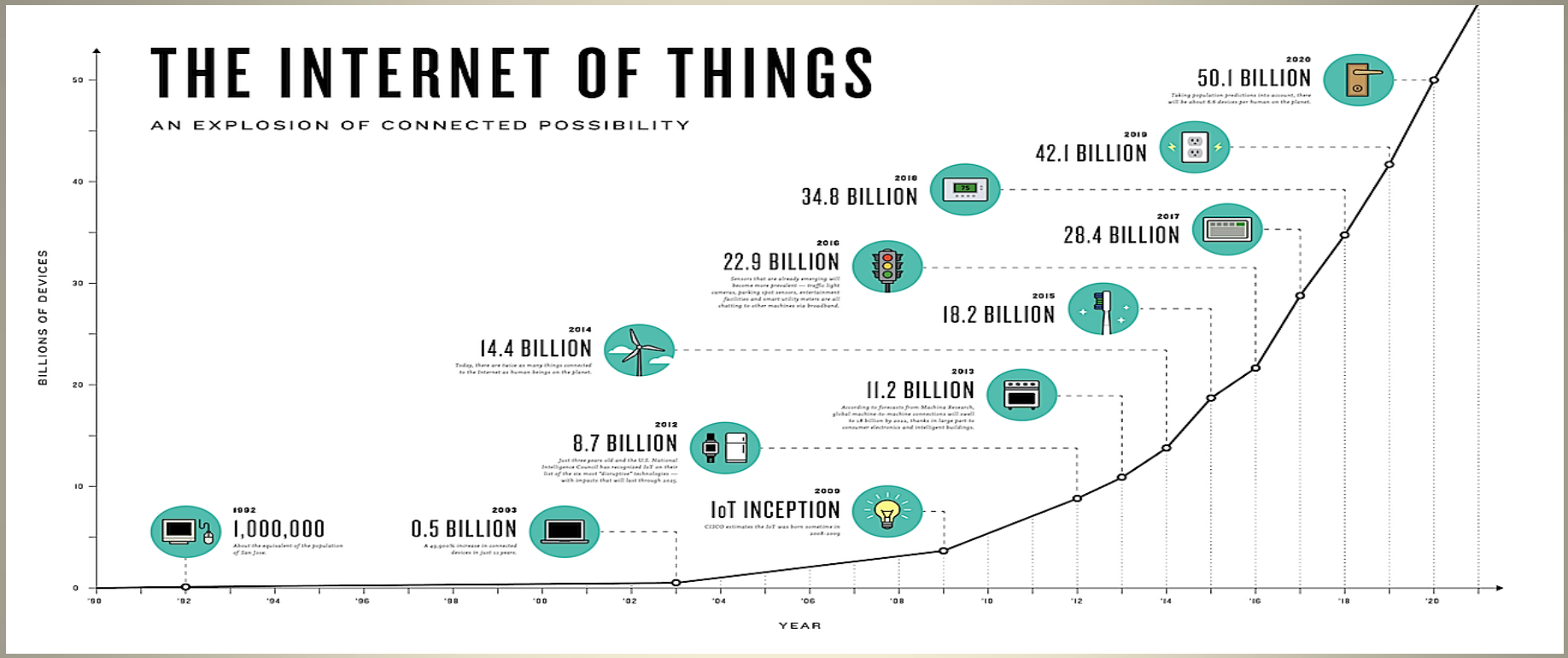
Today's Internet

IoE

1900's

Today

Internet of Things (IoT)



1990 2009 2020

.

Regardless of the exact numbers, one thing is clear: there is much that can still be connected and it's safe to assume we'll probably reach the lower numbers of connected devices (20-35 billion) by 2020.

https://www.ncta.com/platform/industry-news/infographic-the-growth-of-the-internet-of-things

Risk Exposure

Home

Government

Bad Guys

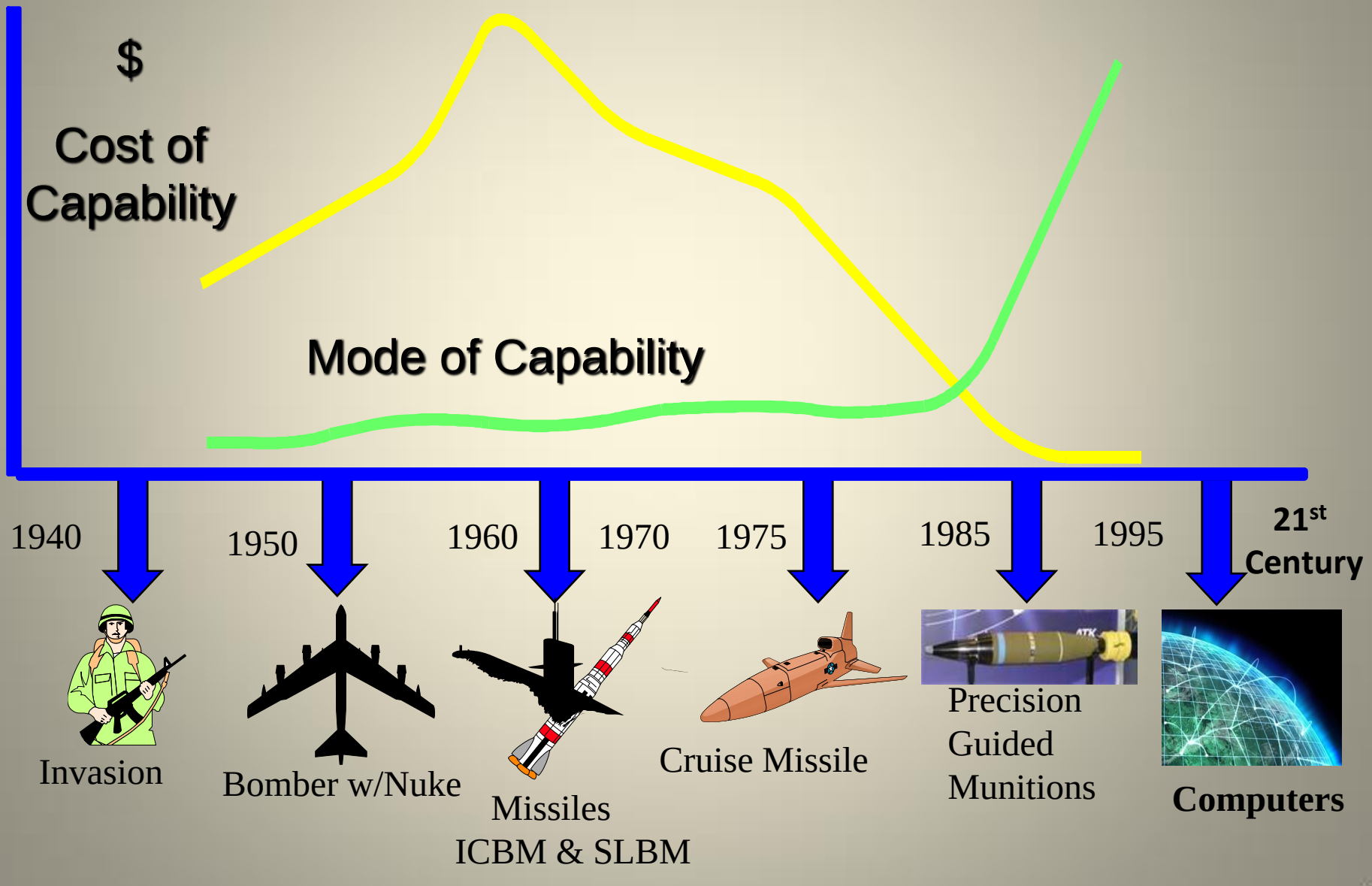
Internet

Business

Military

The World

Cost & Mode of Warfare



What's at Stake

America's Critical Infrastructure

- **Industrial**
  1. Production
  2. Refining
  3. Manufacturing

- **Utilities**
  1. Nuclear
  2. Electrical Grid
  3. Chemical Plants
  4. Gas & Oil
  5. Water
  6. Waste

- **Facilities**
  1. Airports
  2. Ship Yards / Ports
  3. Distribution Centers
  4. Space Stations
  5. Military

Todays Threat Landscape

Discussion Tonight:

1. Phishing Attacks
2. IoE attacks
3. Data Ransom
4. Automobile Attacks
5. China Attacks

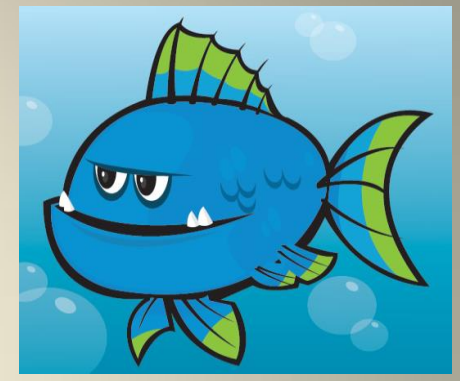
Other Threats:

1. Supply Chain Attacks (Poor security – open back doors)
2. ICS/SCADA attacks (Attacks on U.S. **Critical** Infrastructure)
3. Solar Storms (magnetic storms from the Sun)
4. Cyber Warfare (potential control or destruction of U.S.A critical infrastructures)
   - **Hacking** – **China, Russia, North Korea, Iran, Terrorists, etc.**
   - **EMP Weapons** - Any **electromagnetic pulse** and or disturbance that can destroy, interrupt, obstruct, or otherwise degrade or limit the effective performance of electronics and electrical equipment.

QiWi

1 - Phishing Emails

- Social engineering techniques that persuade you to **download rouge attachments** (Malware), **click** on an **rouge embedded web link** (Malware) and or **make a rouge phone call** (provide PII)



- **What do they want: Money, Data or PII**

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form Links in email

Note: If you dont fill the application your account will be permanently blocked. Threats

Regards,

Facebook Copyrights Department. Popular company

2 - Internet of Things (IoE)

Anything that can Process Information Packets (IP)

- PC's, Desktops, Laptops
- Servers, Network Appliances
- Printer, Copier, Fax, Scanner
- iPads, iPhones
- iGlasses, iWatches

- Home Appliances
- Video Cameras
- Consumer goods
- Anything
- Etc.

Dyn Attack

Dynamic Network Service, Inc. (Dyn)

The first iteration was a free dynamic DNS service known as DynDNS

October 21, 2016 DDoS attack on DNS services at Dyn left 1200 major web sites unreachable for hours.

BotNets

3 - Ransomware

Ransomware is Malware that infects computers, networks and services.

Life Cycle:

Victims computer is infected with Malware

Malware immediately encrypts data HD, and / or systems, making them unreadable

Actor demands payment using digital Bitcoins in order to decrypt files and or your network.

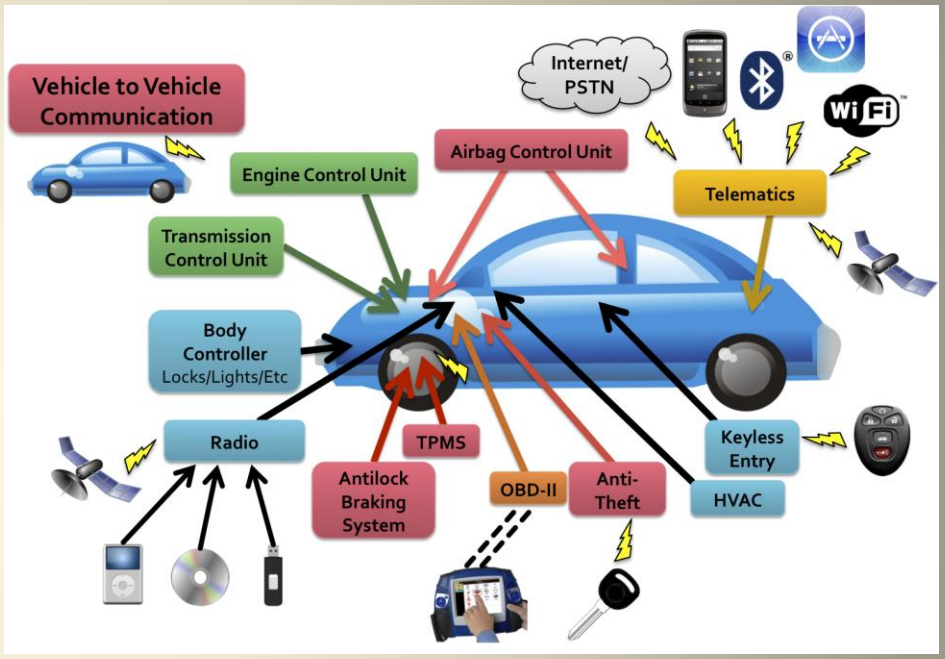
New variants are coming out everyday

Financial Implications

FBI Internet Crime Complaint Center (IC3) data:

4 - Analysis of **Automotive** Attack Surfaces

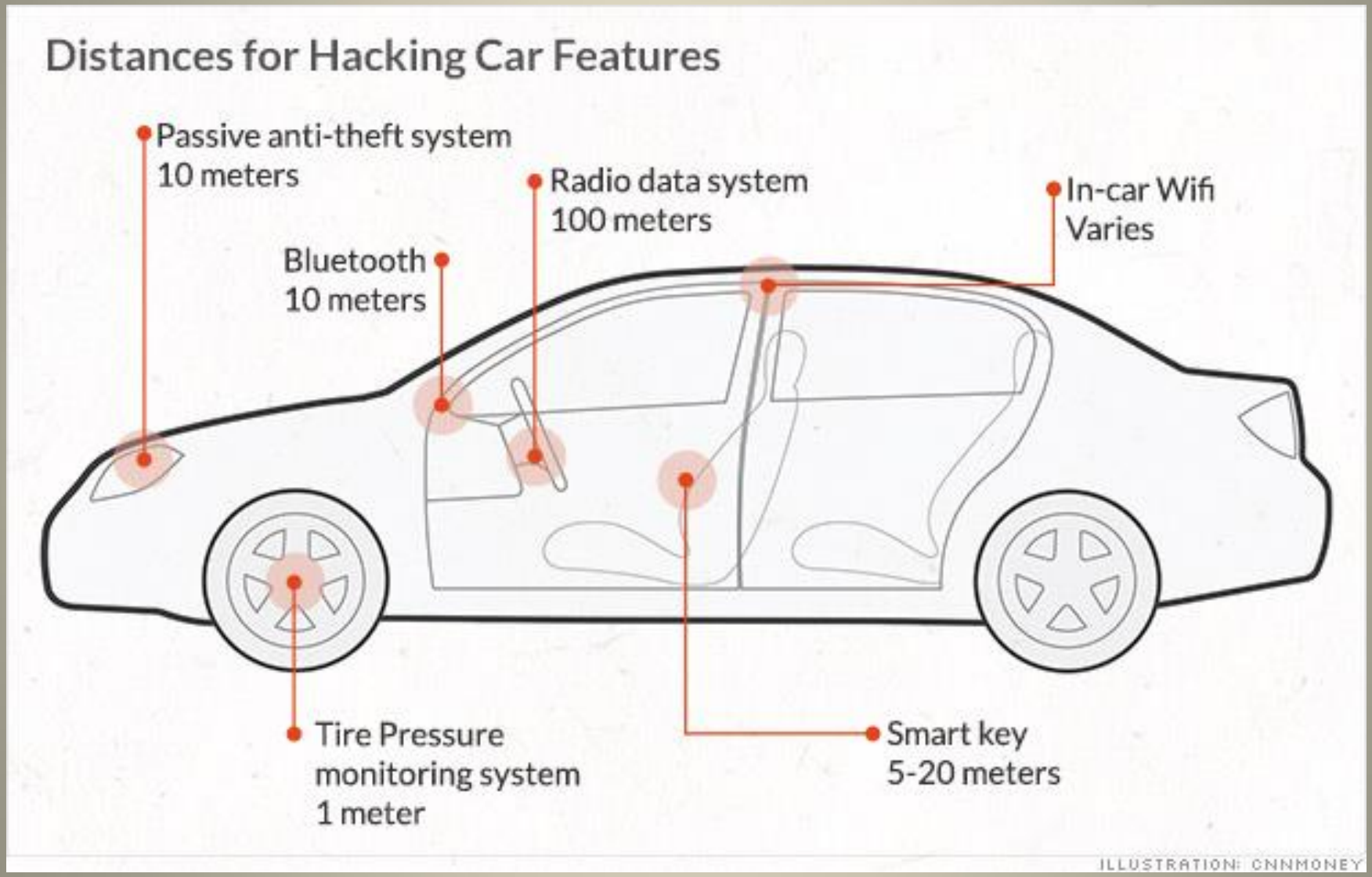
- Modern automobiles are pervasively computerized
  - Engine, Transmission, Body, Airbag, Antilock Brakes, HVAC, Keyless Entry Control, etc.
- Attack Surface extensive
  - Telematics: Blue Tooth, Cellular, Wi-Fi, Keyless Entry
- Attack Surface is easily exploited
  - OBD Diagnostics
  - CD players
  - Bluetooth
- Cellular Radio/ Wi-Fi / ****Satellite**
  - Allow long distance vehicle control, location tracking, in-cabin audio exfiltration



Source: : University of California, San Diego: Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage University of Washington: Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno

Telematics is a method of monitoring a vehicle. By combining a GPS system with on-board diagnostics it's possible to record – and map – exactly where a car is and how fast it's traveling, and cross reference that with how a car is behaving internally.

Could hackers could slam on your car's brakes?



http://money.cnn.com/2014/08/01/technology/security/most-hackable-cars/index.html?hpt=hp_t2

5 - Cyber Attacks by China

June 2015 Attack on OPM and stole massive PII

March 2015 Canadian researchers say Chinese hackers attacked U.S. hosting site GitHub

February 2012 Media reports say that Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters and probably the F-22 Raptor.

December 2011 and June 2012, cyber criminals targeted twenty-three gas pipeline companies & stole info

October 2011 Networks of forty-eight companies in the chemical, defense, and other industries were penetrated

January 2010 Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than thirty other U.S. companies

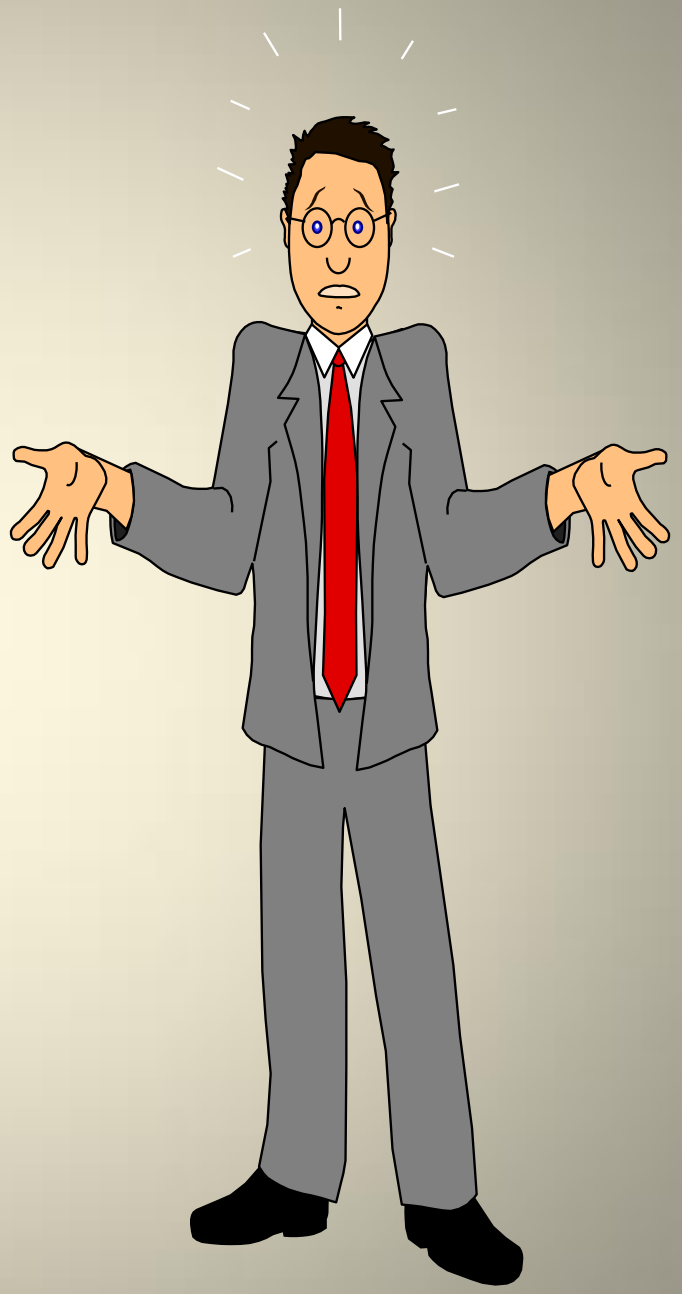
***China targeted GitHub because it was hosting pages for organizations that circumvent its Great Firewall

OPM Attacks by China

Sept. 2016 over 21 million records stolen

We still do not have a National Policy or Plan that defines Cyber Warfare and how we will respond

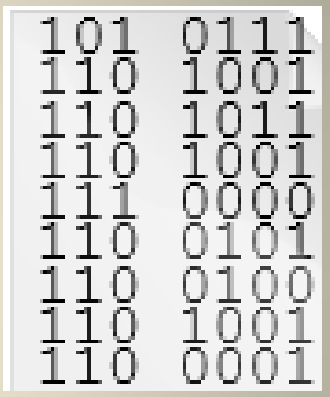
SO HOW DO WE OVERCOME THESE PROBLEMS?



WORKFORCE DEVELOPMENT
Thomas Nelson
COMMUNITY COLLEGE

Understand that You Cannot Protect Everything in Cyberspace…. Therefore Prioritize and Define Your **Crown Jewels**!

- **Information is a critical asset**
  - Government
  - Business
  - Military
  - Personal (legal and financial documents, family photos, etc.)



- **Our failure to protect key information can directly affect**
  - Economic & Marketplace Advantages
  - R&D
  - National Security
  - Warfighters in the field!

21

Cyber Threat Intelligence
2016 Cyber Security Conference

Presented by Thomas Nelson Workforce Development & InfraGard

Featuring: Colonel Jason Sutton,
Director of Communications,
Headquarters Air Combat Command,
Joint Base Langley-Eustis, Virginia.

"Cyber Threat Intelligence," a popular strategy being used in both the military and industry. Cyber threat intelligence is based on multiple layers of information and can be analyzed using the "Cyber Kill Chain" process.

Friday, October 7

Peninsula Workforce Development Center
600 Butler Farm Road, Hampton

Guest Experts:
FBI, FireEye, Raytheon, Verizon & More

Price: $20

Cost includes: continental breakfast, lunch, speakers, wifi, cyber security informative handouts, continuing education units (CEUs) and networking opportunities.

Sign-In - 7 a.m.
Conference - 8 a.m.

Register Today

tncc.edu/workforce

THOMAS NELSON™
The Peninsula's Community College

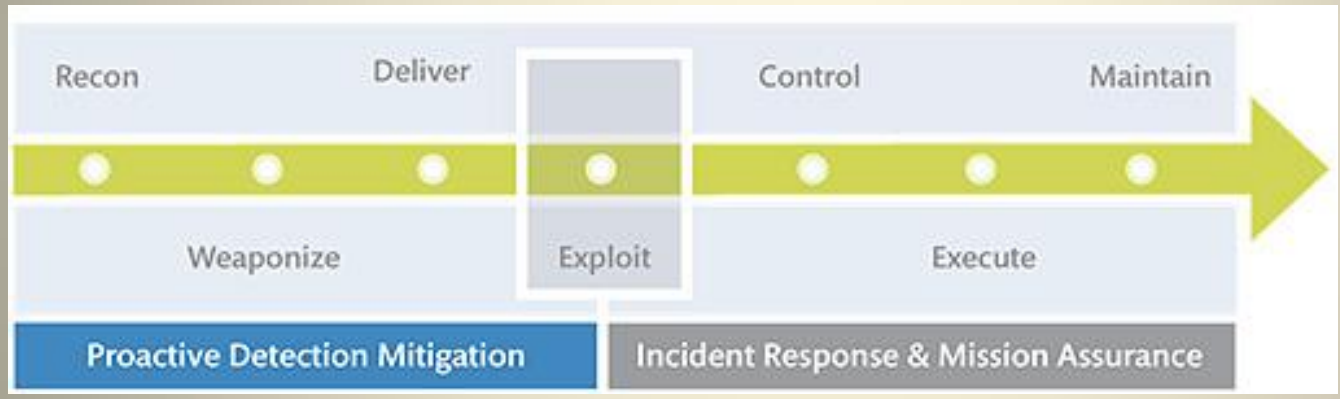
VIRGINIA Peninsula Chamber of Commerce

20th ANNIVERSARY INFRAGARD

Defending Complex Networks

The Cybersecurity Kill Chain and Cyber Attack Lifecycle

Cybersecurity Kill Chain: A sequence of actions performed by an adversary to execute cyber attacks with specific objectives, such as theft of data.



MITRE: Cyber Attack Lifecycle

Cyber Attack Lifecycle: A framework or model to understand and anticipate the moves of cyber adversaries at each stage of the attack.

“Dridex” Kill Chain Analysis:

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Vigilant users	Firewall ACL				
Weaponization	Deploy Spam Filters	Direct to Junk Folders	AV			
Delivery	Vigilant users	Deploy Policy Lockdown Macros	AV	Message Queuing		
Exploitation	IPS HIDS	Sandbox emails	Deploy DEP			
Installation	IPS HIDS	HIDS	AV			
Control		Firewall ACL		Tarpitting Spammers	DNS Sinkhole	
Execute	Audit logs			QoS	Honey Pot	
Maintain	Update antivirus	Update IPS/HIDS	Change Passwords	Update Firewall ACL		

Security for Home & Personal Networks

- Develop a good Cybersecurity **"Attitude"**
- **Use Common Sense and be a role model**
- Know that security measures are not 100%
- Assume you have been already Hacked

Home Security Measures:

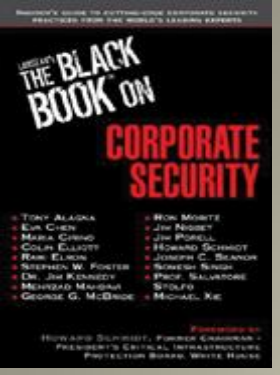
- Use your PC in the **"Limited User Mode"**
- ID your most important data and store it off-line: example USB Drive
- Back up your USB drive weekly **(use encryption)**
- Install Router / Firewall between your COX Cable Modem and your Home Network
- Install Anti-Virus / Firewall suite on your PC Operating System O/S
- Keep O/S, Router/FW and Anti-Virus/FW up to date with the latest patches (weekly)
- Disable MS Macro features (instead use Word Viewer in MS Office emails)

"Be Cybersecurity Vigilant"

Security for Home & Personal Networks

- Never open suspicious emails and or click on embedded Web links **(Phishing)**
- Maintain an encrypted vault for all your passwords and change regularly
- **Verify** that **you use (HTTPS://)** in the URL window, especially when conducting any financial business on-line
- Do not download anything from **untrusted** web sites
- Reconsider using mobile devices for on-line financial transactions
- Do not use airport, restaurant, hotel, Cyber Café and or Public use PC's **for your financial transactions**
- Keep a separate PC for children to use
- When you think you are Hacked "**Air Gap"** your PC and begin the remediation process

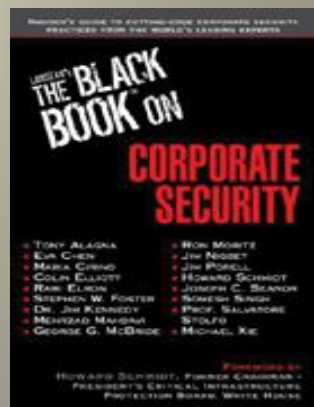
"Be Cybersecurity Vigilant"



"The Seven Pillars of Cybersecurity"

It's a Continuous Process

1. Recognize the Importance of Securing our Digital Infrastructure **(Attitude)**
2. Cultivate Management Support, i.e. Board of Directors and C-Suite
3. Develop Meaningful Cybersecurity Policies (Enforcement)
4. Develop a Workable Cybersecurity Framework (NIST or ISO)
5. Implement a Robust Cybersecurity Awareness Program
6. Conduct Continuous Education and Training for Information Systems Users
7. Conduct Regular Cybersecurity Audits and Network Assessments



****By Contributing Author, Stephen W. Foster, 2005**

What Should Cyber Citizens Do

Everyone's to Do List

- Recognition that our National Digital Infrastructure is a "National Security Priority"
- Support Passage of Congressional Legislation to protect U.S Information Systems
- **Develop a strong Cyber Security mind set and attitude**
- **Practice safe computing and encourage others to do the same**
- **Continue your education and training on Cyber Security – be aware!**

WORKFORCE DEVELOPMENT
Thomas Nelson
COMMUNITY COLLEGE

Contact Info and Questions

Steve Foster, FBI, ret., CISSP

Cybersecurity Project Director
Professor
Lecturer

Thomas Nelson Community College
Historic Triangle Campus
Workforce Development Team

fosters@tncc.edu

757-258-6600