MVCC
MOHAWK VALLEY COMMUNITY COLLEGE

Cybersecurity Threat Landscape

Jake Mihevc
jmihevc@mvcc.edu

My Background

- Dean- Science, Technology, Engineering, and Math.
- Director, NSA CAE Regional Resource Center
- M.S. in Cybersecurity, Utica College
- Security+, Network+

MVCC
MOHAWK VALLEY COMMUNITY COLLEGE

CENTERS OF ACADEMIC EXCELLENCE
CAE

UTICA
COLLEGE

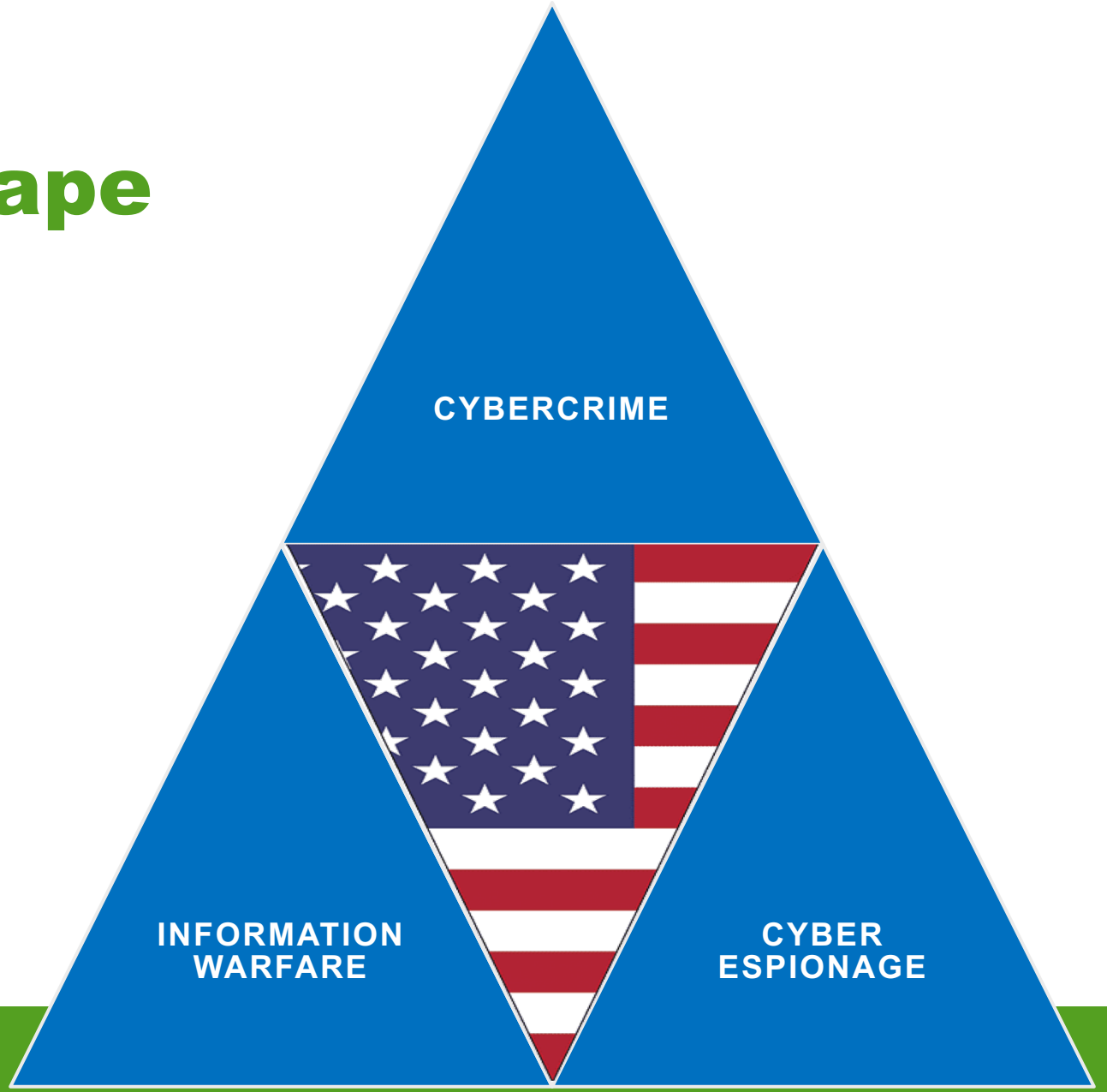
CompTIA Network+ CERTIFIED

CompTIA Security+ CERTIFIED

Disclaimer

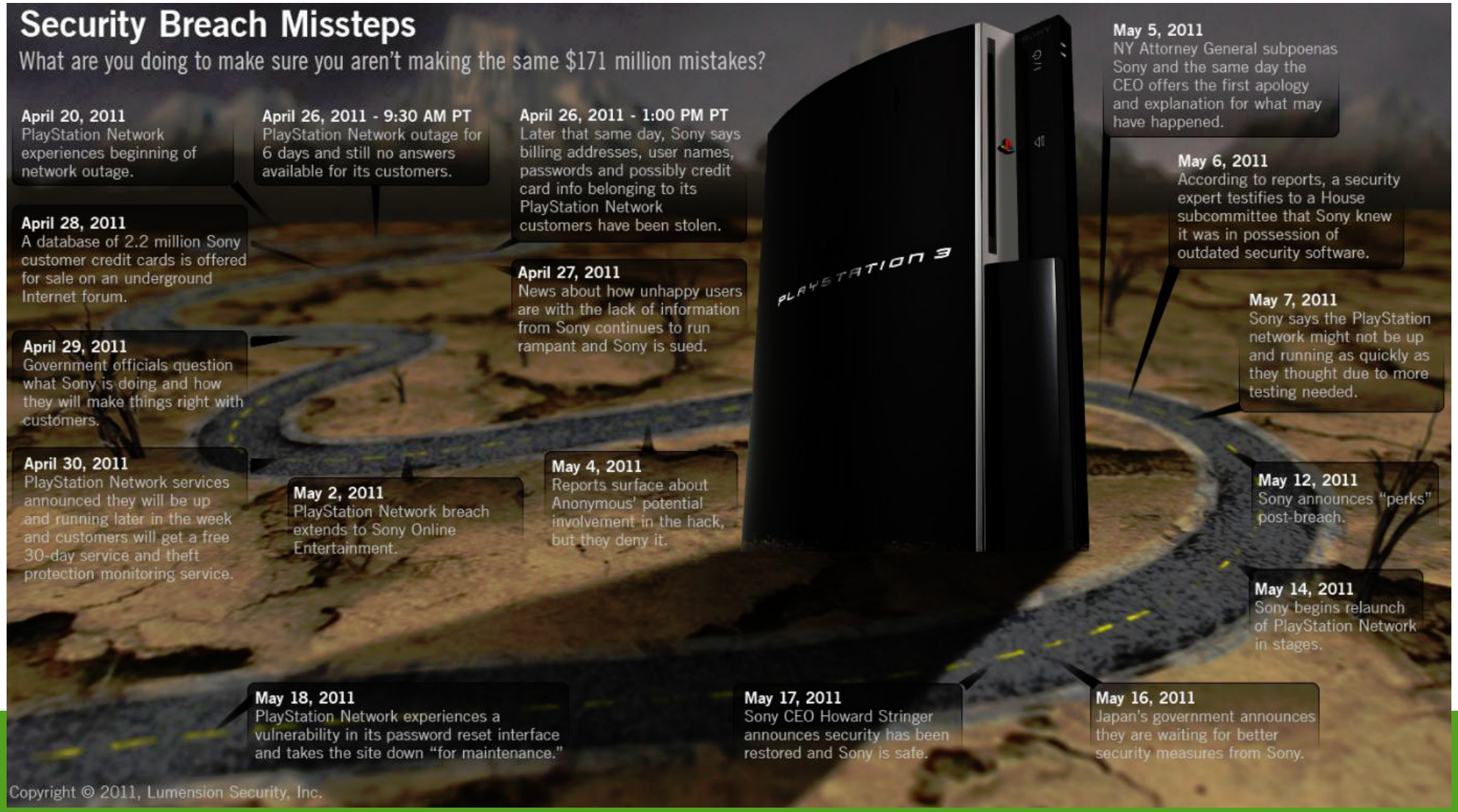
- The Views expressed in this presentation are my own, and may not reflect the positions or views of MVCC, the NSA, or any other institutions with which I am affiliated.

Threat Landscape

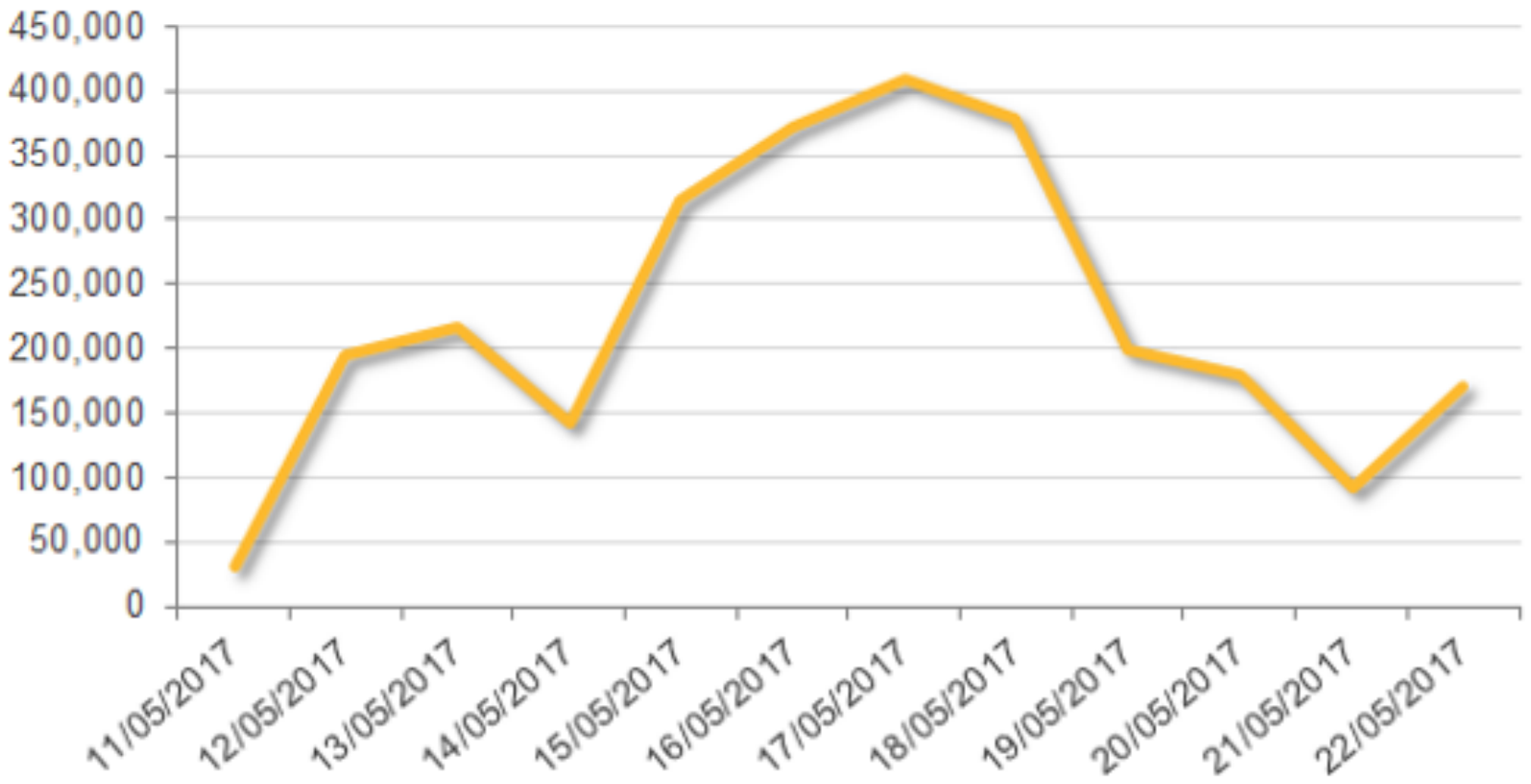



IF I COULD GET GOOD NEWS INSTEAD OF BAD NEWS
THAT WOULD BE GREAT

CyberCrime-Playstation Network Hack

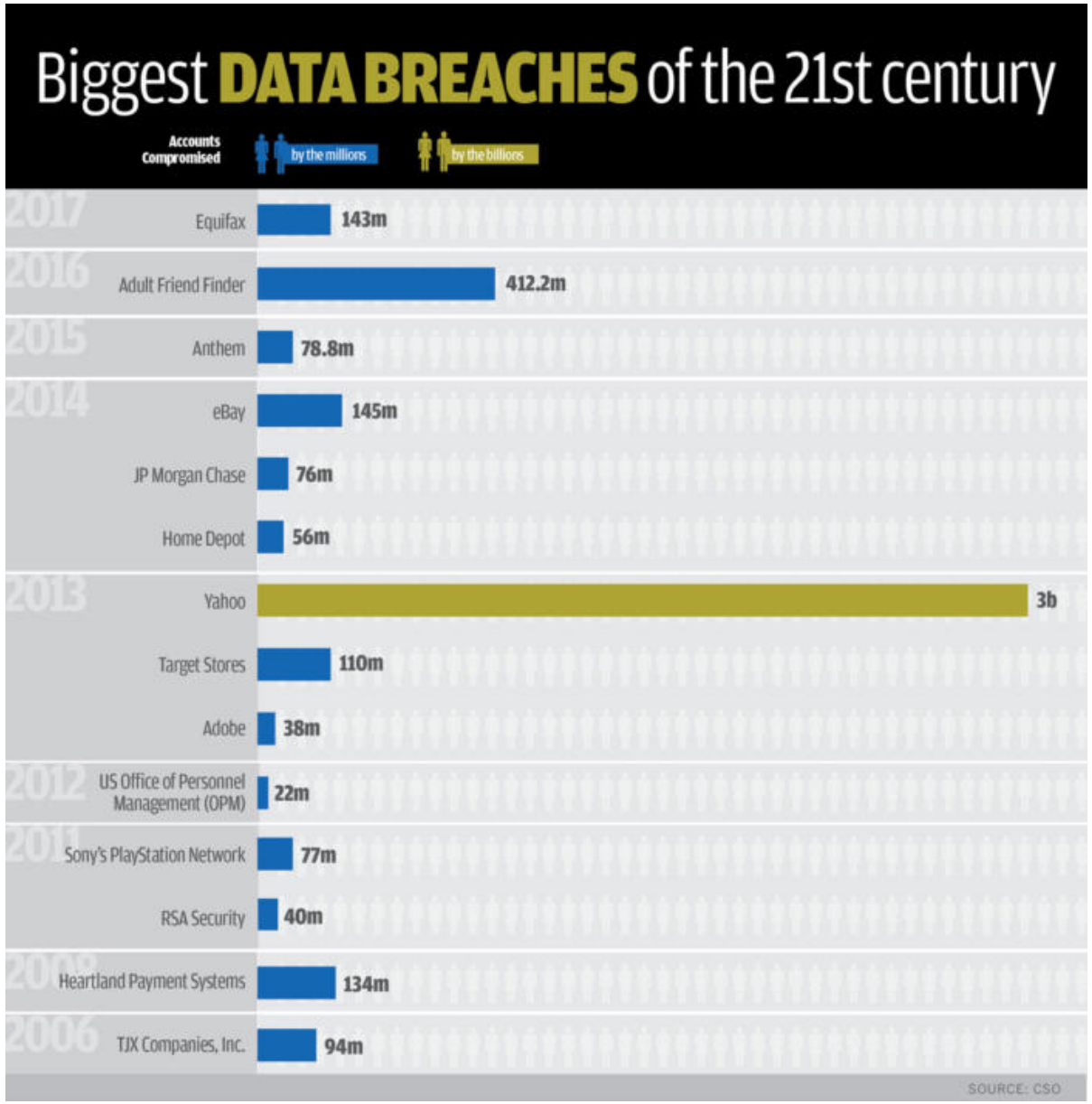


CyberCrime-WannaCry Ransomware



Proliferation of Ransomware

- October 04, 2019 - The FBI released an alert this week about an increase in ransomware attacks across all sectors, including healthcare, state and local governments, and other infrastructure targets. **Ransomware attacks have do**ubled in 2019.
- Ransomware attacks against at least **621** government agencies, healthcare providers and schools in the first nine months of 2019, **largely without repercussions.**
- The **FBI: victims should not pay the ransom** because it does not guarantee an organization will regain access to its data.
- **Paying ransoms emboldens criminals** to target other organizations and provides an alluring and lucrative enterprise to other criminals.
- Your insurance company: **PAY THE RANSOM**
- Some victims who paid a ransom were never provided with decryption keys.
- Due to flaws in the encryption algorithms of certain malware variants, **victims may not be able to recover some or all of their data even with a valid decryption key**.


Biggest DATA BREACHES of the 21st century
Accounts Compromised
by the millions
by the billions
2017
Equifax
143m
2016
Adult Friend Finder
412.2m
2015
Anthem
78.8m
2014
eBay
145m
JP Morgan Chase
76m
Home Depot
56m
2013
Yahoo
3b
Target Stores
110m
Adobe
38m
2012
US Office of Personnel Management (OPM)
22m
2011
Sony's PlayStation Network
77m
RSA Security
40m
2009
Heartland Payment Systems
134m
2006
TJX Companies, Inc.
94m
SOURCE: CSO

Equifax Data Breach

EQUIFAX

- Unpatched software led to the exposure of credit data on 145.5 million customers.
- 30 back doors identified
- Question: Are there any negative repercussions for Equifax?

Cybercrime- Data Breaches

- Data is the “exhaust” of the Information age
- Worldwide, we create more data per day than we did from the beginning of time until 2004.
- “ You have zero privacy anyway. Get over it.” –Scott McNealy, CEO of SUN Microsystems, 1999.
- “Privacy is obsolete, only people your age think it exists” –Proctor High School Student, Summer 2013

Information Warfare

Oil Pipeline- Turkey, 2008

Information Warfare

The saga of Ukraine since 2014 illustrates the Russian blueprint for future cyberwar.

Ukraine Chronology

2004 Presidential race:

Pro-Russian Viktor Yanukovych's **Pro-Western Viktor Yushchenko.**

-Yuschenko Survives poisoning two weeks before the election and wins.

-Ukraine is Pro-Western for six years.

Yushchenko poisoning, sound familiar?

Ukraine Chronology

2010 Presidential race:

Pro-Russian Viktor Yanukovych's **Pro-Western Yulia Tymoshenko.**

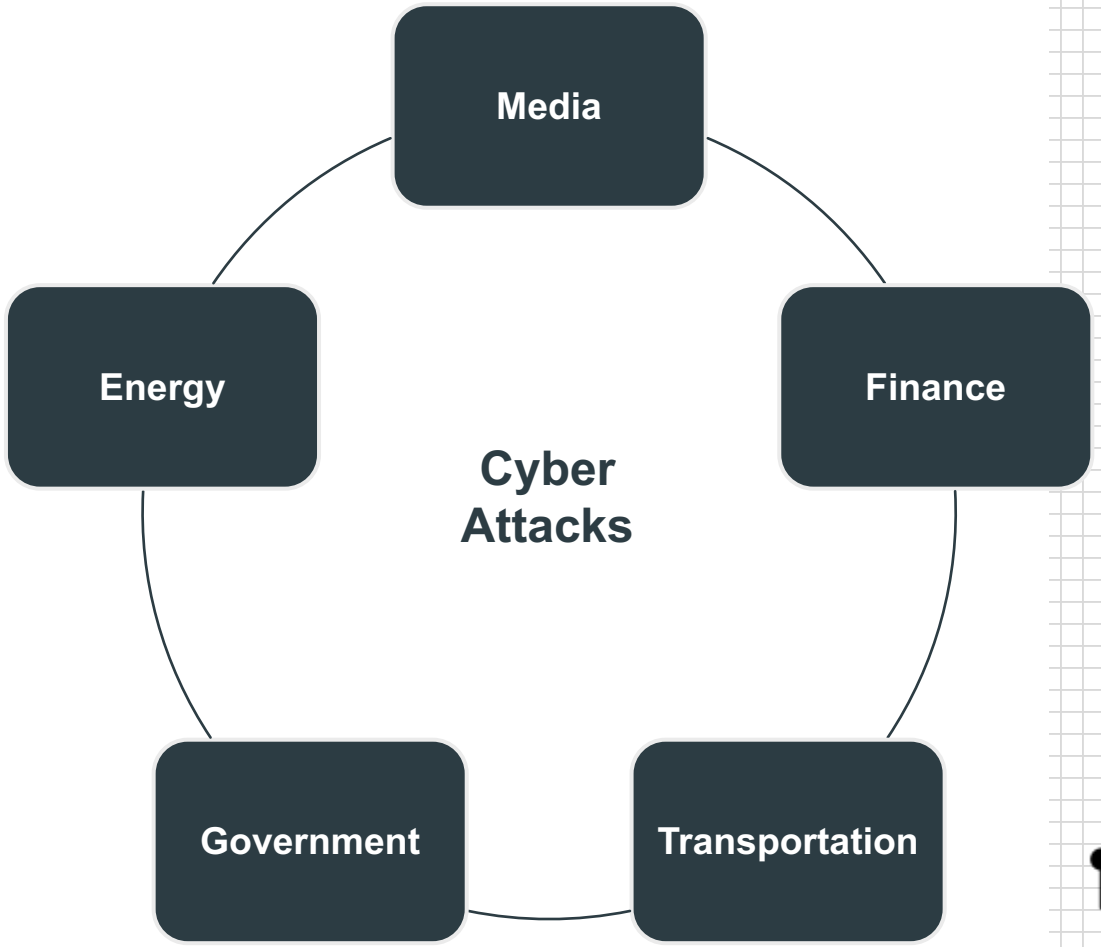
-Yanukovych wins and serves until 2014.

-Withdrawal from alignment with EU/NATO in 2014 Sparks the Ukrainian Revolution.

- Yanukovych flees to Russia, Paul Manfort returns to the US having advised Yanukovych from 2004-2014.

Ukraine Chronology

- Yanukovych government is overthrown in February of 2014.
- Russia invades and annexes Crimea in April.
- Russia launches persistent and effective cyber attacks on Ukrainian Critical Infrastructure
- Two 12-hour long **blackouts** in 2015 and 2016 affecting 100,000 people are attributed to Russian hackers.
- Ukranian Finance Ministry loses terabytes of financial data to KillDisk as they prepare the budget in August 2016.



Information Warfare

- Ukraine moves government web presence to a hosting service located in the United States.
- The attacks continue….is this an act of war against the United States?
- Common attack signature is identified:
- **BlackEnergy** Trojan delivers the
- KillDisk Payload.
- *Identical signature found within American power and water utilities in 2014.*

Information Warfare: EU Targets

- Two days before France's presidential run-of in May 2017, malicious hackers leaked nine gigabytes of e-mails from candidate Emmanuel Macron's campaign onto the web.
- In Germany, questions arise over the lack of Russian interference in Sept 2017 election after May 2015 hack of 16GB of Bundestag e-mails and documents.

Information Warfare: US Target

- In the United States, Bots proliferate on Social Media focusing on divisive issues such as gun control, race relations, and pro-choice/pro-life positions in Late 2015/ Early 2016
- In the months leading up to the November 2016 election focus shifts to promote Republican candidate.
- USC Researcher Emilio Ferrera finds that 20% of Twitter content in the four weeks prior to the election was generated by 50 million bots.
- Emergence of “Computational Propaganda”

Information Warfare: US Target

- Clinton Campaign Chairman John Podesta and DNC Staffer fall victim to a phishing campaign.
- Private emails and confidential documents appeared online day after day — procured by Russian intelligence agents, posted on WikiLeaks and other websites.

Information Warfare

Stuxnet: The Good Guys Strike Back!

Air Force Research Lab - Rome NY

AIS
Assured Information Security, Inc.

CACI
EVER VIGILANT®

BAE SYSTEMS

SRC

Booz | Allen | Hamilton

ANDRO
Computational Solutions, LLC

ISSI
Intelligent Software Solutions

ITT

CUBRC
Advantage Through Technology

EVERIS
The Cornerstone of Network Security

NORTHROP GRUMMAN

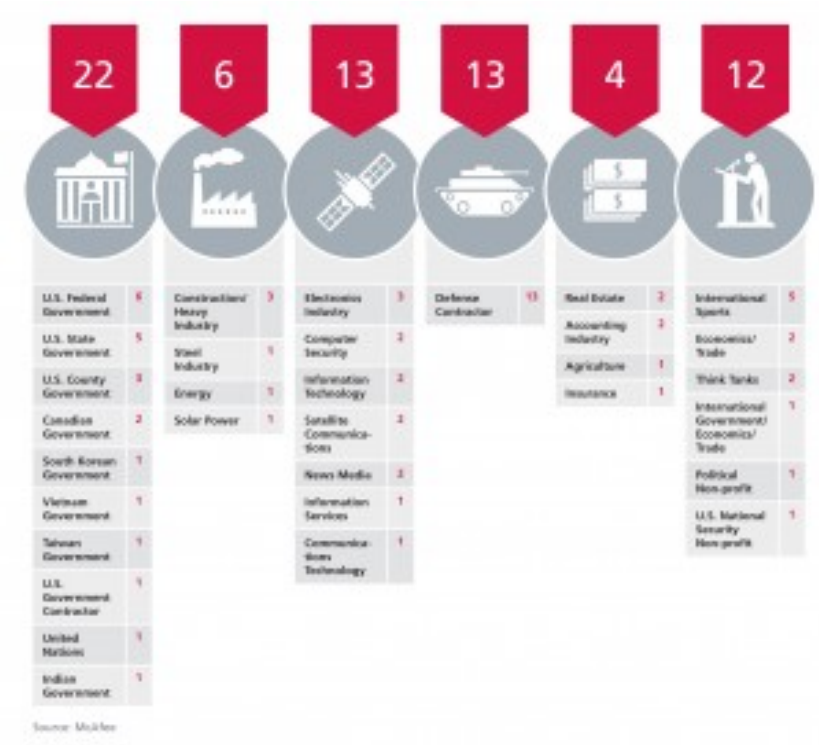
CyberEspionage-China

- PLA Unit 61398 attacked at least 1,000 domestic companies since 2016 and successfully breached at least 141.
- Average breach time 356 days, longest breach time 1,764 days.
- Primary compromise method is Spear Phishing.

PLA Unit 61398

CyberEspionage-China

Operation Shady RAT



CyberEspionage-China

China debuts the J-31 on December 26, 2016.

CyberEspionage-China

CyberEspionage- Secure Supply Chain

- “Pivoting” within a network has now expanded to pivoting between networks.
- Interconnected supply chains especially vulnerable due to “trust” relationships.
- Trust relationships manifest through:
- VPNs “Island Hopping”
- Websites “Watering Holes”
- E-mail “Reverse Business E-Mail Compromise”

- DoD Gets Serious in Q4 of 2018.

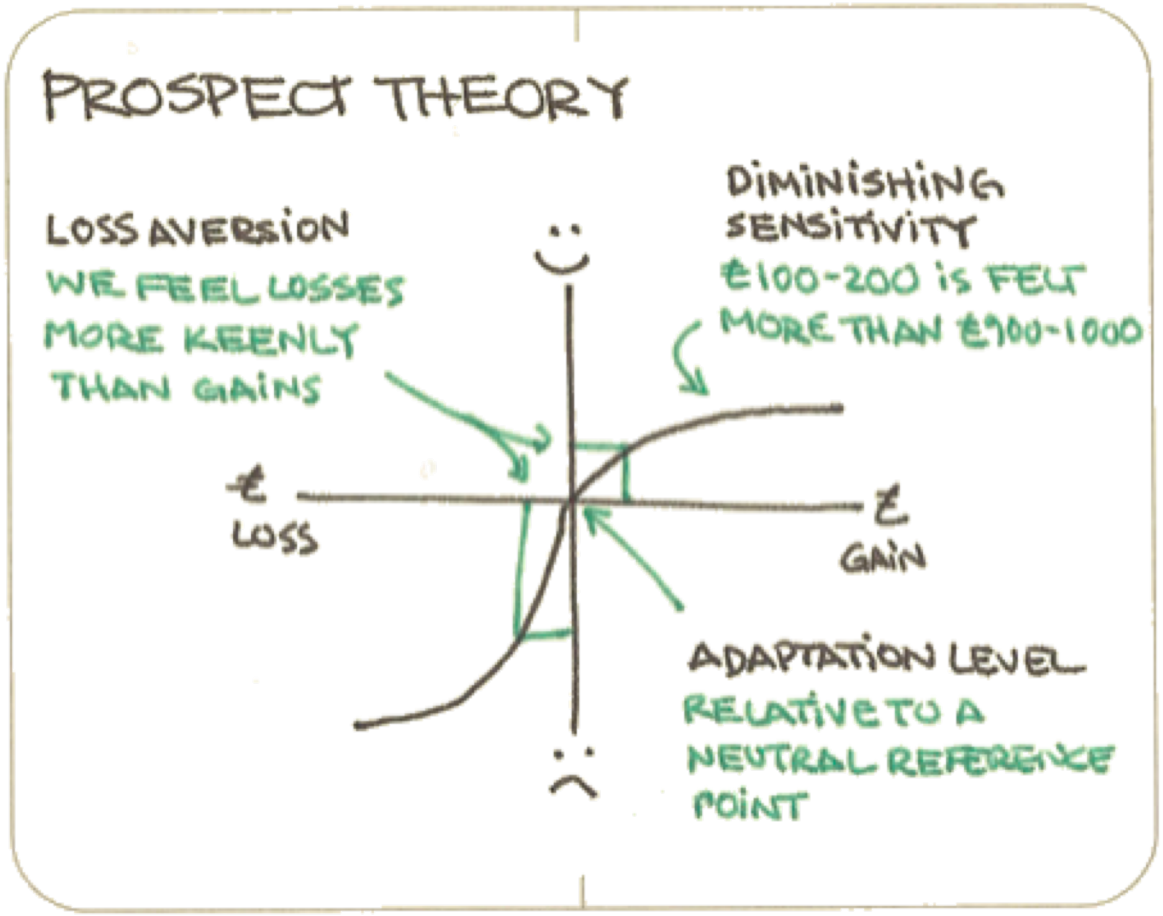
Secure Supply Chain- CIR

- Destruction of logs
- Secondary command-and-control server (C2) used on a sleep cycle
- Increased use of Steganography

Underinvestment in Cyber Defenses

- **Prospect Theory** by *Daniel Kahneman*, Nobel Prizewinner in Economics.
  - Given a choice to receive a **guaranteed $500** or a **50/50 chance for $1000**, what would you choose?
  - Confronted with a **guaranteed loss of $500** or a **50/50 chance to lose nothing**, what would you choose?

Prospect Theory



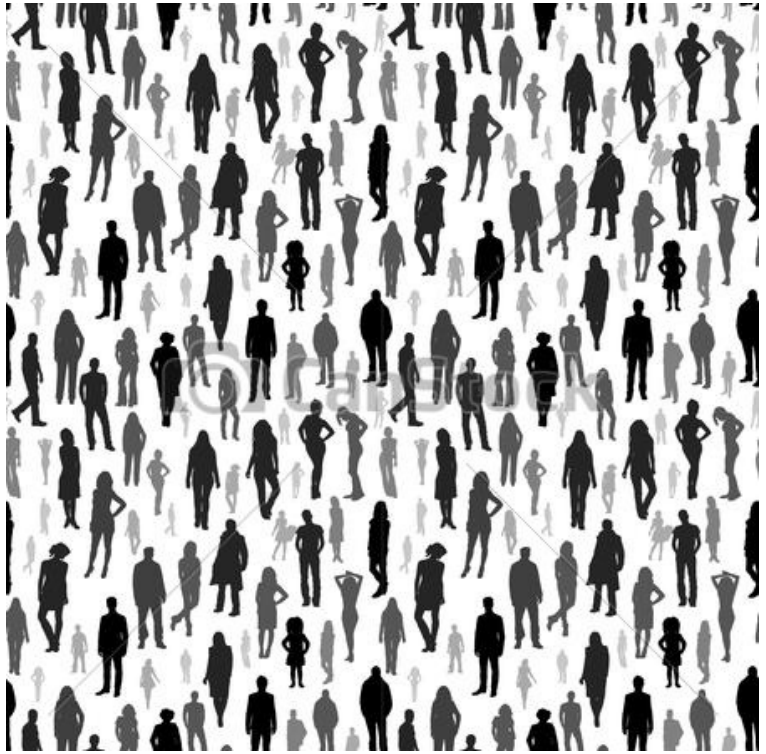
Underinvestment in Cyber Defenses

- US spends $13 Billion on USS Gerald Ford, contracts for two more aircraft carriers at $14 Billion and $15 Billion each.
- Out of a $716 Billion federal defense budget, $15 billion authorized for cybersecurity-related activities (2%).
- Mr. Trump's homeland security adviser, Thomas P. Bossert, who oversaw cybersecurity policy, was dismissed after John R. Bolton took over as national security adviser.
- The cybersecurity coordinator at the White House, Rob Joyce, left his post and returned to the National Security Agency to run the most elite of the US cyberforces.
- The White House lost its two most senior, and most knowledgeable, cybersecurity policymakers in the span of a few weeks in April of 2018. Neither has been replaced.

Workforce Shortage

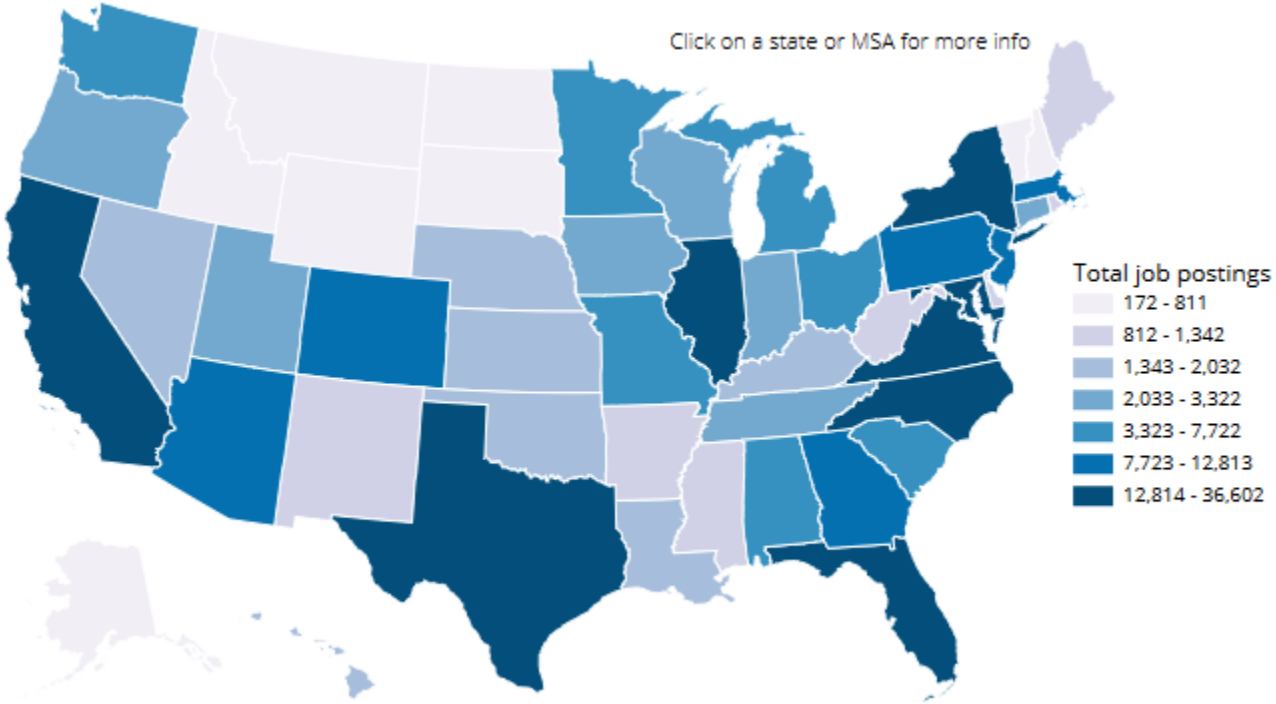
FORCES OF GOOD

FORCES OF EVIL



Workforce Shortage

- 306,000 unfilled cybersecurity positions Nationwide
- Roughly 10,000 existing positions within the Federal Government are currently unfilled.



Cyber Security jobs

Sort by:
relevance - date

Salary Estimate

$70,000	(31855)
$90,000	(24829)
$100,000	(19492)
$110,000	(13617)
$125,000	(6739)

Job Type

Full-time	(38151)
Contract	(3153)
Part-time	(1295)
Commission	(377)
Temporary	(375)
Internship	(150)

Location

Washington, DC	(2175)
New York, NY	(1090)

Upload your resume - Let employers find you

Page 1 of 40,772 jobs

Cyber Security Analyst, Entry/Junior Level
Brockwell Technologies, Inc. (BTI) ★★★★☆ 3 reviews
Huntsville, AL
HBSS (Host Based Security Solution). EMASS (Enterprise Mission Assurance Security System). The position requires daily interaction with the JBC-P cybersecurity...
Easily apply
Sponsored save job

Information Security Analyst I - CSOC Analyst
TD Bank ★★★★☆ 5,076 reviews
Mount Laurel, NJ
Information Security Certification or Accreditation an asset. Participate in security management strategy and framework development....
Sponsored save job

Cyber Security Architect
Florida Crystals Corporation ★★★☆☆ 133 reviews
West Palm Beach, FL 33401
The Cyber Security Architect/Threat Intelligence position reports to the VP of Information Security. Works with security peers, Infrastructure, BASIS, Partners...
Sponsored by **ASR Group/Domino Sugar** save job

Save jobs and view them from any computer. ✕

ttps://www.indeed.com/q-Cyber-Security-jobs.html# Create account (it's free)

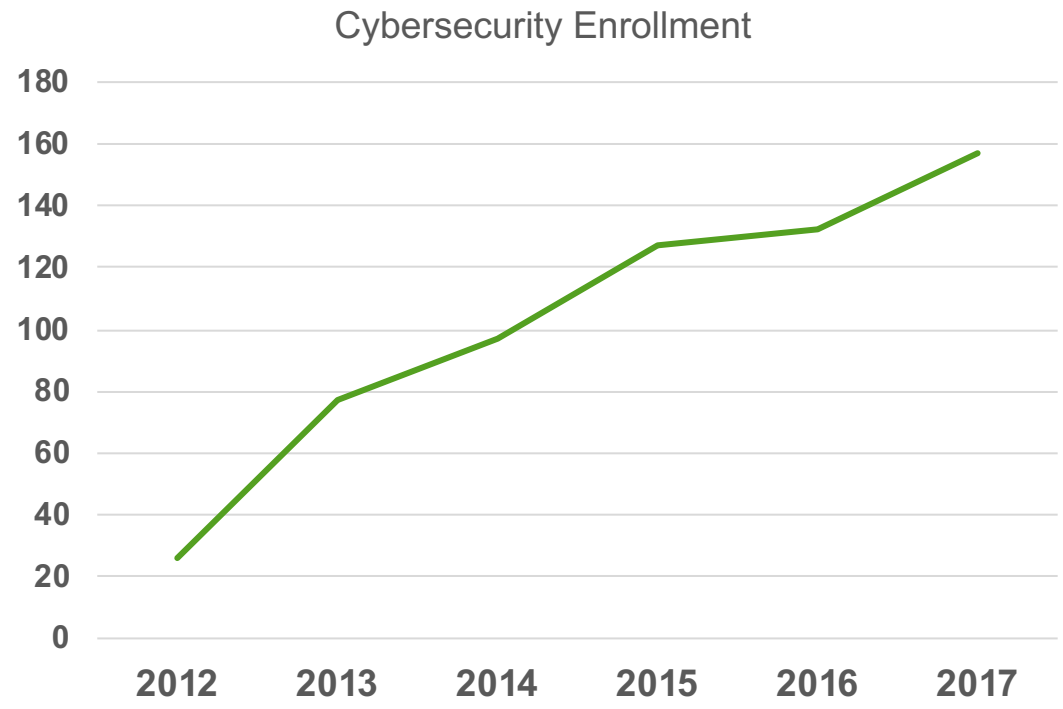
40,772
Open Cybersecurity Positions

Results of Talent Shortage- Government

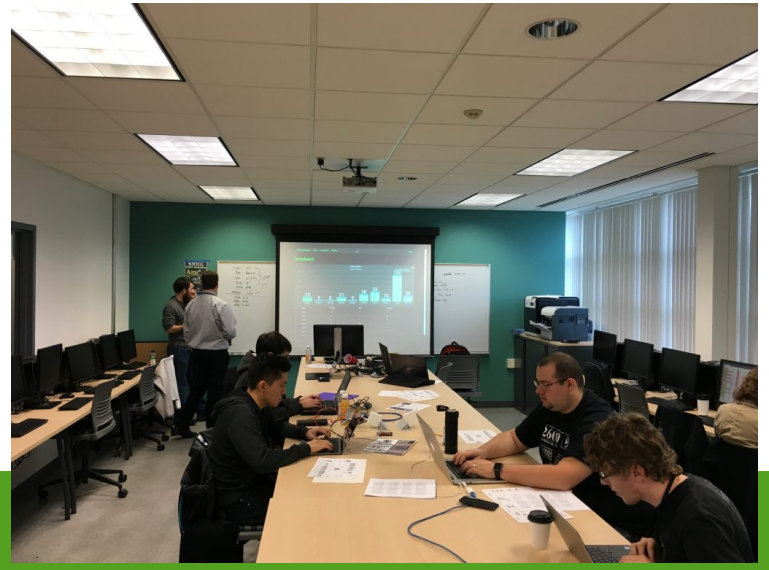
- Shadow Brokers penetrate the Equation Group and auction tools and zero-days.
- Wikileaks release of CIA Vault 7 including weaponized zero-days and malware.
- Deep Root analytics exposes aggregated voter data of 198 million US voters.
- **Office of Personnel Management** hack exposes SF-86 clearance forms.
- Cybercriminals have launched ransomware attacks against at least 621 government agencies, healthcare providers and schools in the first nine months of 2019, largely without repercussions.

Cybersecurity at MVCC

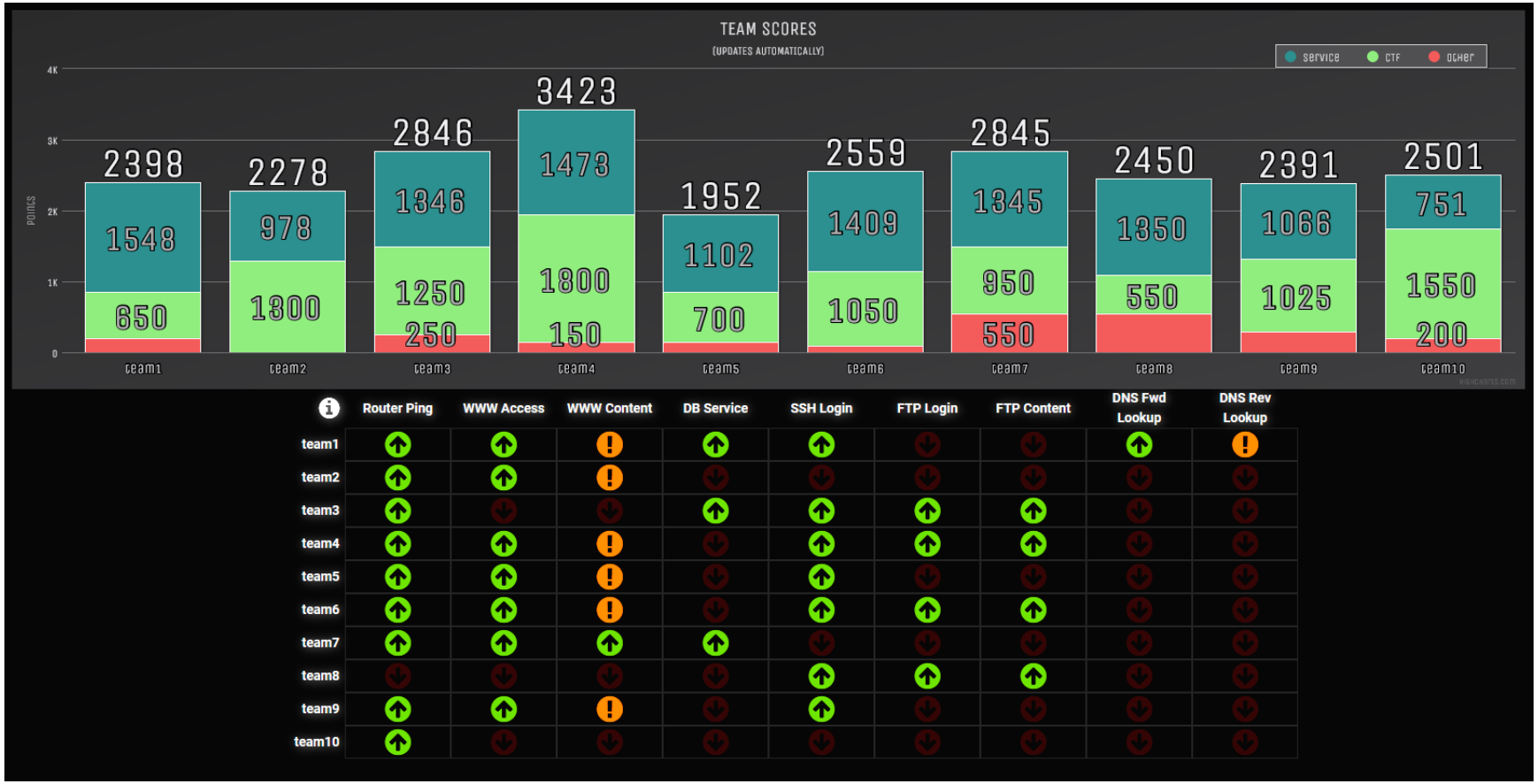
- Designated a Center of Academic Excellence in Cyber Defense by the National Security Agency and Department of Homeland Security in 2016. One of 40 Community Colleges Nation-Wide.
- One of 5 Regional Resource Centers (Northeast) for 240 CAE Institutions.



CNY Hackathon



CNY Hackathon



	Router Ping	WWW Access	WWW Content	DB Service	SSH Login	FTP Login	FTP Content	DNS Fwd Lookup	DNS Rev Lookup
team1	↑	↑	!	↑	↑	↓	↓	↑	!
team2	↑	↑	!	↓	↓	↓	↓	↓	↓
team3	↑	↓	↓	↑	↑	↑	↑	↓	↓
team4	↑	↑	!	↓	↑	↑	↑	↓	↓
team5	↑	↑	!	↓	↑	↓	↓	↓	↓
team6	↑	↑	!	↓	↑	↑	↑	↓	↓
team7	↑	↑	↑	↑	↓	↓	↓	↓	↓
team8	↓	↓	↓	↓	↑	↑	↑	↓	↓
team9	↑	↑	!	↓	↑	↓	↓	↓	↓
team10	↑	↓	↓	↓	↓	↓	↓	↓	↓

Takeaways

- Significant threats from CyberCrime, Information Warfare, Cyber Espionage
- U.S. leads in developing advanced tools and cyber weapons, not enough boots-on-the-ground.
- Small manufacturers have a limited attack surface, investment in secure practices and threat intelligence may mitigate most exposure.