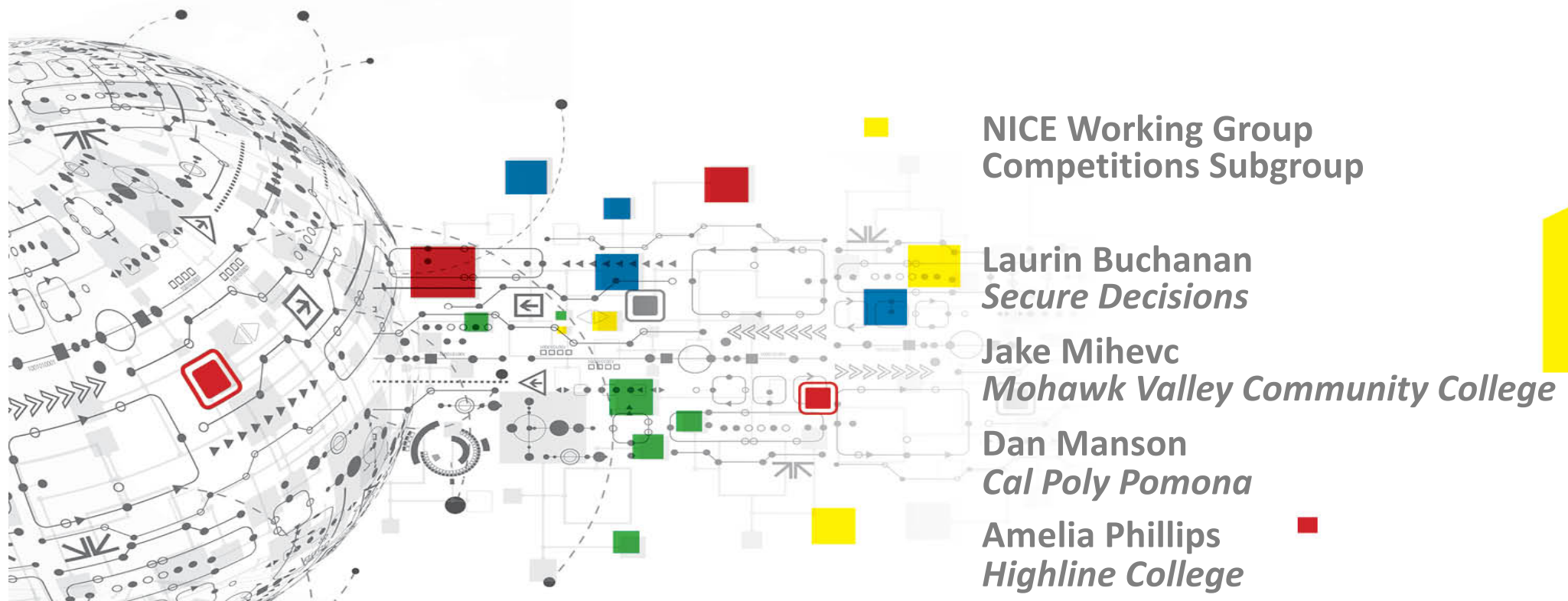


Play Your Way to Success:

Building Tomorrow's Workforce



**NICE Working Group
Competitions Subgroup**

**Laurin Buchanan
*Secure Decisions***

**Jake Mihevc
*Mohawk Valley Community College***

**Dan Manson
*Cal Poly Pomona***

**Amelia Phillips
*Highline College***

NIST NICE Working Group (NICEWG)

Provides mechanism in which public and private sector participants can

- develop concepts
- design strategies
- pursue actions that advance cybersecurity education, training, & workforce development

3 Co-Chairs: Academia, Industry, Government

5 Sub-Working Groups



NICEWG Competitions Sub-Group Mission/Vision

Vision:

Promote a spectrum of competitions that advances knowledge, skills and abilities to nurture and expand a diverse national talent pool.

Mission:

Empower a public and private competition ecosystem by providing guidelines, standards, and best practices for players, teams, schools, sponsors and organizers.



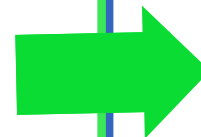
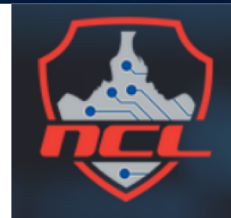
Competitions and games come in all flavors



K-12

Collegiate

Workforce





Case Study: Attracting interest in cyber careers



What: introducing kids to cyber issues and roles

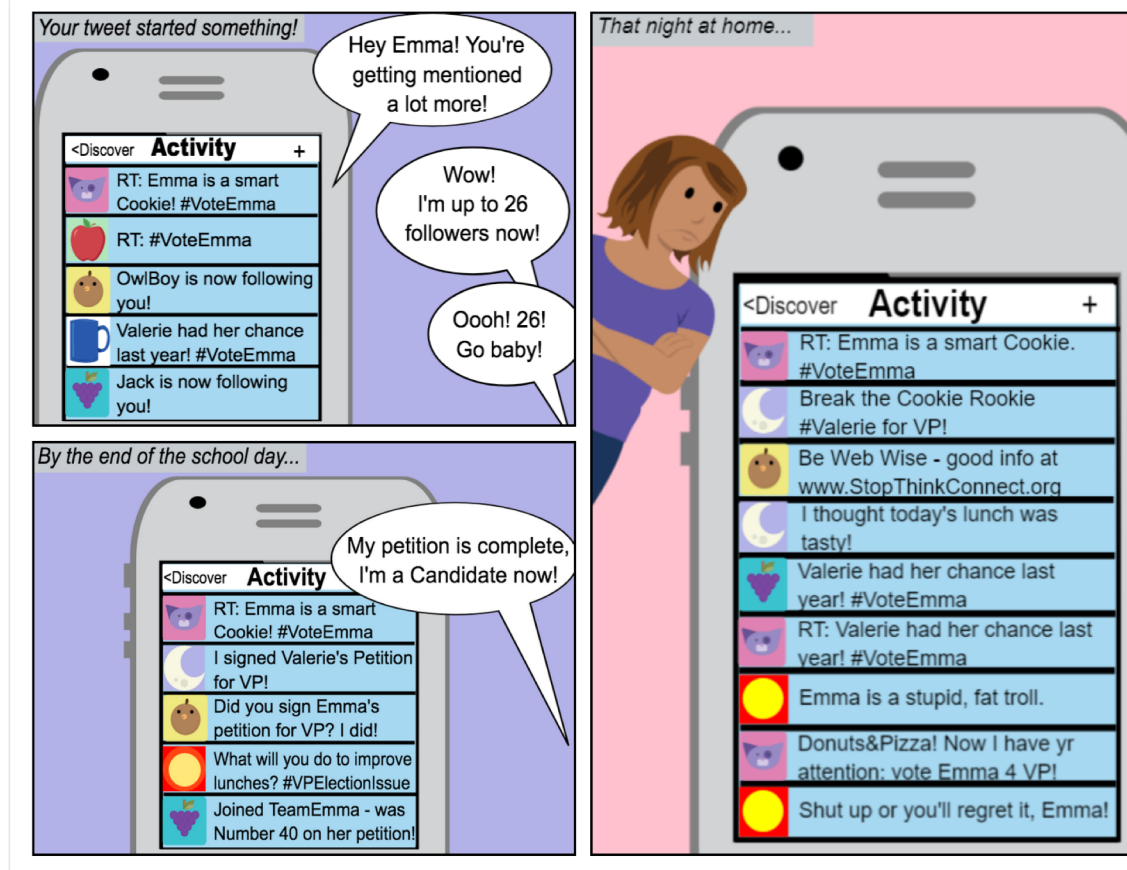
Who: Middle school kids

Where: Community center

When: After school

How: Branching web comics show how cybersecurity affects everyone

Why: Get kids interested in cyber



We only found one piece of malware at FirstBank, on a manager's computer.

But every malware has a unique "signature" - like fingerprints - that tells us about it. We can use that to find other incidents with this malware.

Ding!
Analysis complete

NBI Malware Analysis System Signature Report

Submitted by: Melissa Adrien
Case: FirstBank
Filename: %Temp%\iexplore.exe

MALWARE TYPE

General Trojan: .08% = No
Banking Trojan: .05% = No
Virus: 0% = No
Worm: 0% = No
Ransomware: .02% = No
Rootkit: 0% = No
Common: 40% = Yes
(spam, spyware, adware)

Hmmm,
this malware doesn't do anything special.
This doesn't tell us much!

[CLICK HERE TO VIEW CHOICES](#)



NBI Malware Analysis System
Signature Report

Submitted by: Melissa Adrien
Case: FirstBank
Filename: %Temp%\iexplore.exe

MALWARE TYPE

General Trojan: .08% = No
Banking Trojan: .05% = No
Virus: 0% = No
Worm: 0% = No
Ransomware: .02% = No
Rootkit: 0% = No
Common: 40% = Yes
(spam, spyware, adware)

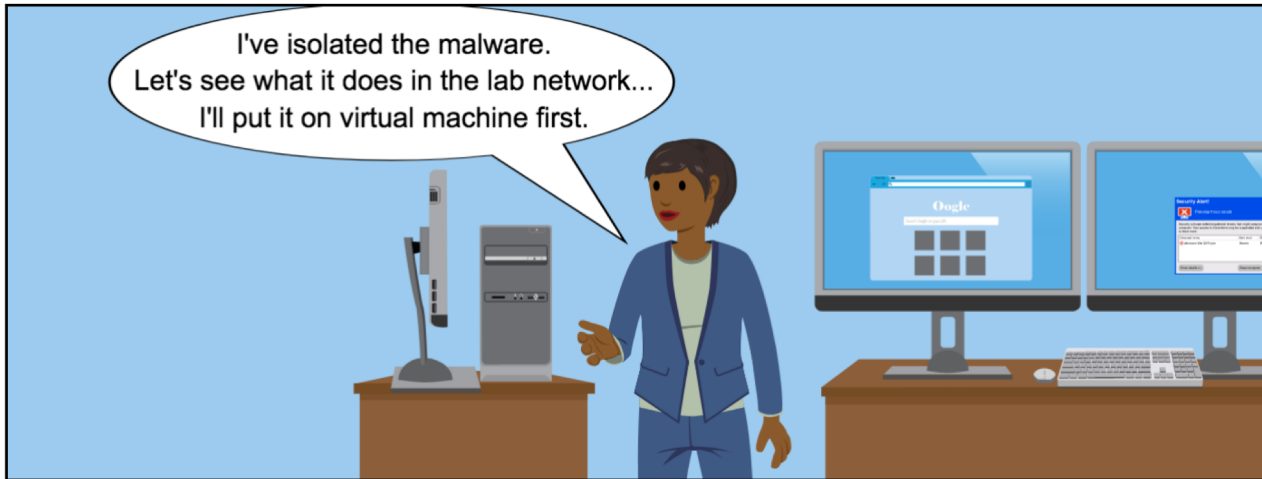
*Hmmm,
this malware doesn't do
anything special.
This doesn't tell us
much!*

How do you learn more about the malware?

Try to run the malware in the lab

Look for similar malware in other investigations

[CLICK HERE TO VIEW CHOICES](#)



OK - sometimes malware doesn't trigger in a virtual machine.
I'll try a physical machine.

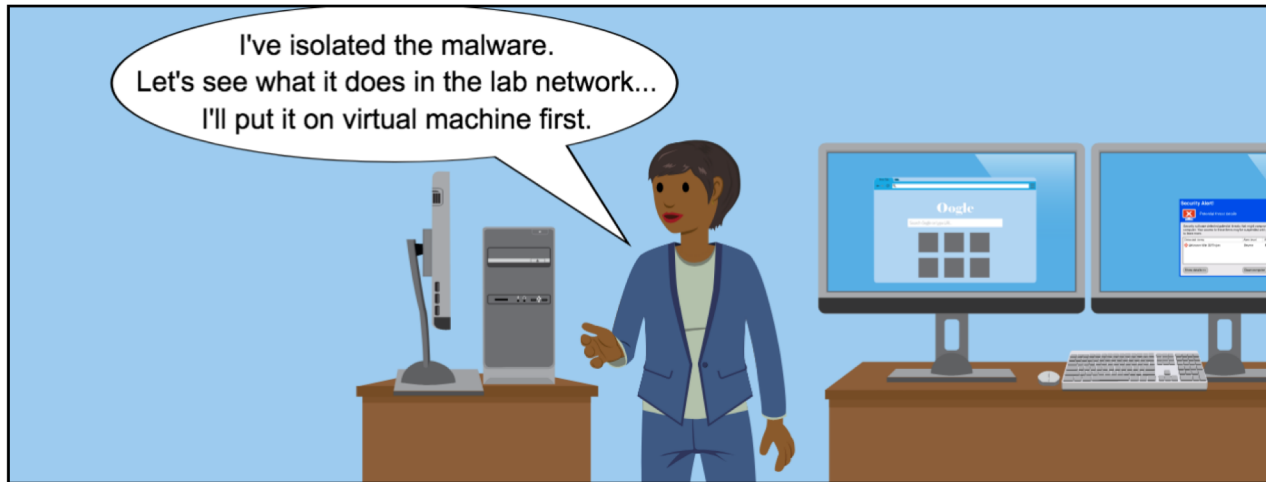
Virtual Machine (VM) Analysis System Report

08:00 - Scan: no malware detected
08:10 - VM reboot
08:23 - Scan: no malware detected
08:30 - VM reboot
08:35 - Scan: no malware detected

This malware just isn't doing anything.
What am I missing?

Forensic Framework System Analysis Report

10:01 - Scan: no malware detected
10:10 - VM reboot
10:28 - Scan: no malware detected
10:35 - VM reboot
10:49 - Scan: no malware detected



OK - sometimes malware doesn't trigger in a virtual machine. I'll try a physical machine.

Virtual Machine (VM) Analysis System Report

- 08:00 - Scan: no malware detected
- 08:10 - VM reboot
- 08:23 - Scan: no malware detected
- 08:30 - VM reboot
- 08:35 - Scan: no malware detected

This malware just isn't doing anything. What am I missing?

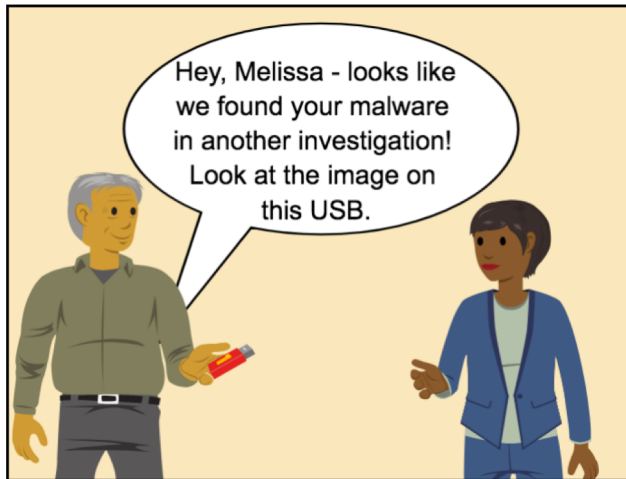
Forensic Framework System Analysis Report

- 10:01 - Scan: no malware detected
- 10:10 - VM reboot
- 10:28 - Scan: no malware detected
- 10:35 - VM reboot
- 10:49 - Scan: no malware detected

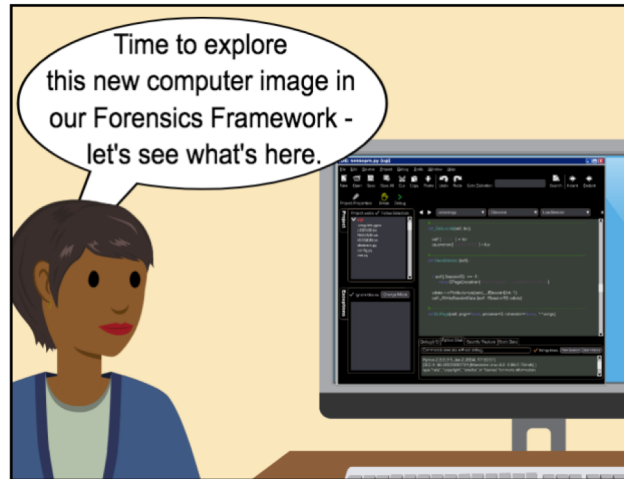
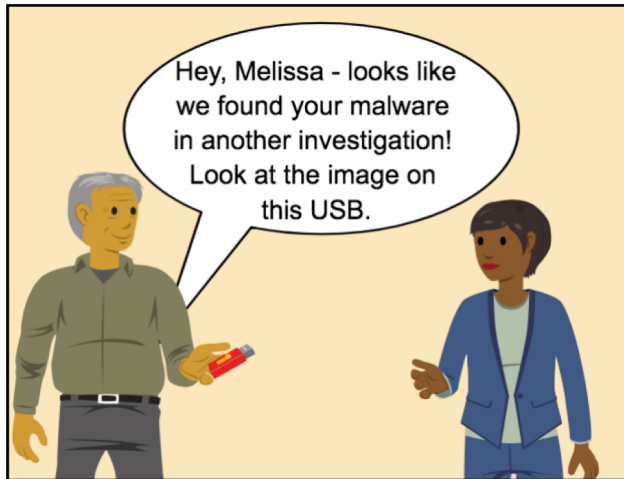
So that didn't work - what do you want to try next?

Analyze systems of FirstBank's customers

Look for this malware in other investigations



[CLICK HERE TO VIEW CHOICES](#)



How do you expand your investigation to include this new .dll file?

Ask malware specialist to analyze the .dll file

Look for the .dll file in the images you have from the bank and its customers

Look for that .dll file in any other recent investigation

Web comics are popular with everyone

Positive “first contact” experience is critical to continued interest in next stage

- Learn while having fun
- Literally “see yourself” in comics
 - critical for developing self-efficacy

Go beyond reading comics: much deeper engagement when learners create their own comics

Roles and Their Job Descriptions



Forensics Analyst:

Like a detective, looks for evidence of what happened in a cyber crime or attack: data left behind that may explain who did it and how.



Cyber Crime Investigator: Leads teams of different cyber experts to investigate cyber crimes, generally in law enforcement.



Cyber Defense Forensics Analyst:

Analyzes evidence from cyber attacks to design safeguards that can detect or prevent that method from being successful again.

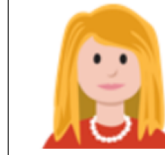


Cyber Defense Incident Responder: Responds quickly to minimize damage from cyber attacks at his company, like a fireman putting out a fire.



Cyber Defense Analyst:

Implements and monitors defenses to keep a company's data, network and systems secure from known cyber attacks and to quickly detect new attacks.



Cyber Security Manager: Manages people and efforts to keep her company's data, systems and network safe and protected.



Malware Analyst:

Analyzes malware like viruses, worms, bots, rootkits, and Trojans to understand how they work.



Threat Analysis Specialist: Researches and analyzes attackers, their motives and attack methods, to understand the threat they pose to organizations.

Failure always an option - and bigger is better with comics!



Memorable or exaggerated endings reinforce learning

Story format shows consequences of choices immediately: not bound by reality of time and distance

Experience consequences of bad decision in a safe environment



Case Study: Competitions as part of formal education

Mohawk Valley Community College (MVCC)

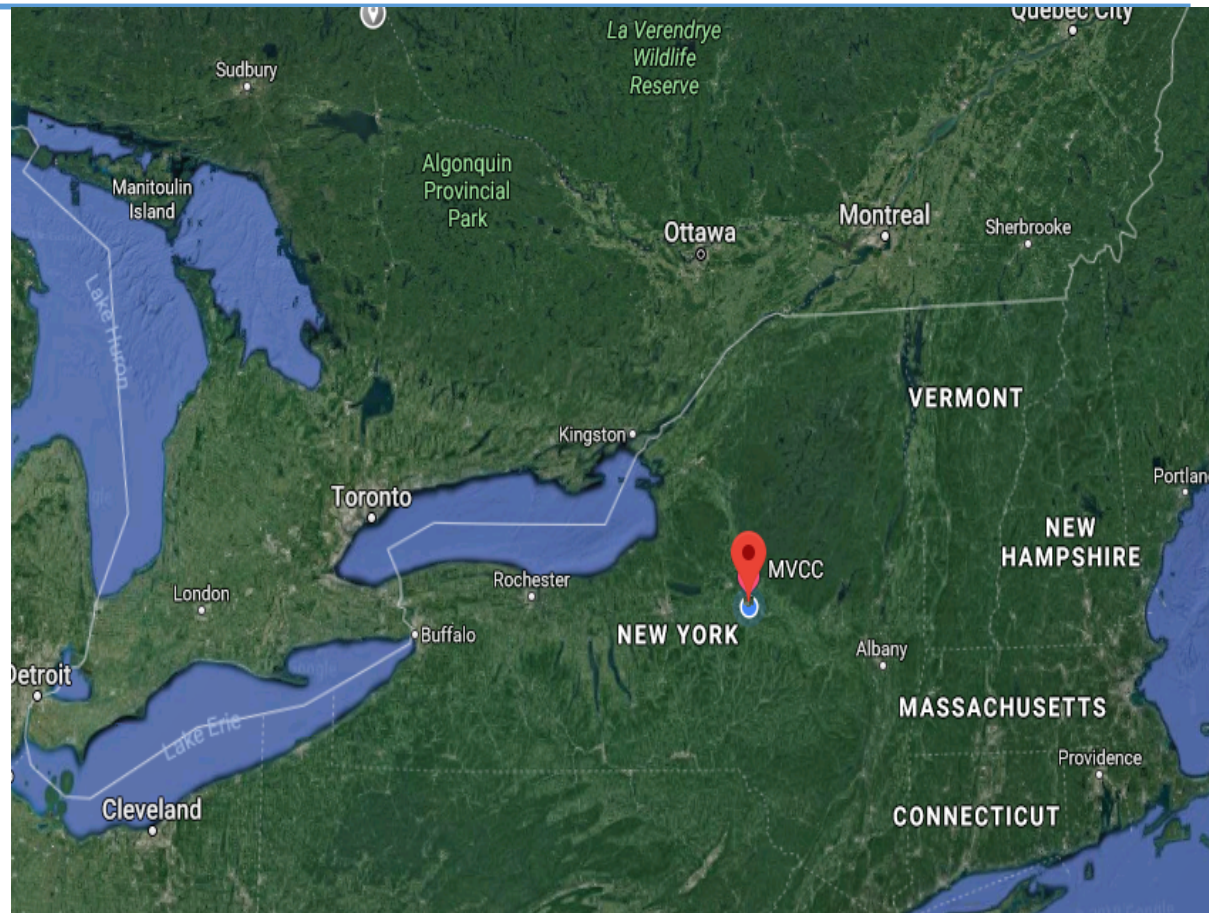
MVCC: CAE 2Y

Utica College: CAE-CDE

SUNY Polytechnic

Air Force Research Lab in
Rome, NY

**Central New York (CNY)
Hackathon: 1 event each
semester**



CNY Hackathon

8 different colleges participate

Teams composed of students from each college

Competition elements

- Infrastructure (CCDC)
- Capture The Flag (CTF)
- Wireless Challenge



Friday and Saturday, Nov. 3 and 4
Mohawk Valley Community College Utica Campus

Kickoff Event Friday

4-5 p.m. Lightning Talks:
"Blue Whale Challenge Investigation: What your mobile device knows about you," Josh S. White, Ph.D., Secure Mind Analytics
"Designing your own tools: The Amass Pen-Testing Tool," Jeff Foley, ClaritySec

5-6 p.m.
Dinner and Introduction to Main Event Challenges

6-9 p.m.
CNY Hackathon Classic Competition Kali vs. Metasploitable. Teams to compete to own services in the competition environment

Main Event Saturday

8:30 a.m. - 5 p.m. Saturday
CNY Hackathon Competition:
Defend Services from Red Team Attacks, Capture the Flag, Wireless Challenges, and more.

Hosting Schools:
MVCC UTICA
MOHAWK VALLEY COMMUNITY COLLEGE COLLEGE

Platinum Sponsors:
GRIFFISS INSTITUTE, AIR FORCE STEM, QUANTERION SOLUTIONS INCORPORATED, LE MOYNE (Greatness meets Goodness), BNY MELLON | Invested

Gold Sponsors:
nycm INSURANCE, PARO Government

Direct all questions to
Jake Mihevc at jmihevc@mvcc.edu



Competitors develop more than technical skills

Soft skills:

- Leadership
Team Leaders – HANDS OFF
- Teamwork
Teams created by script

Students learn WHY they need to learn networking, operating systems and coding so well

Students are engaged

Students learn where they stand -
need to work harder?



Students WANT to come back better
next year

Benefit to MVCC goes beyond enrollment

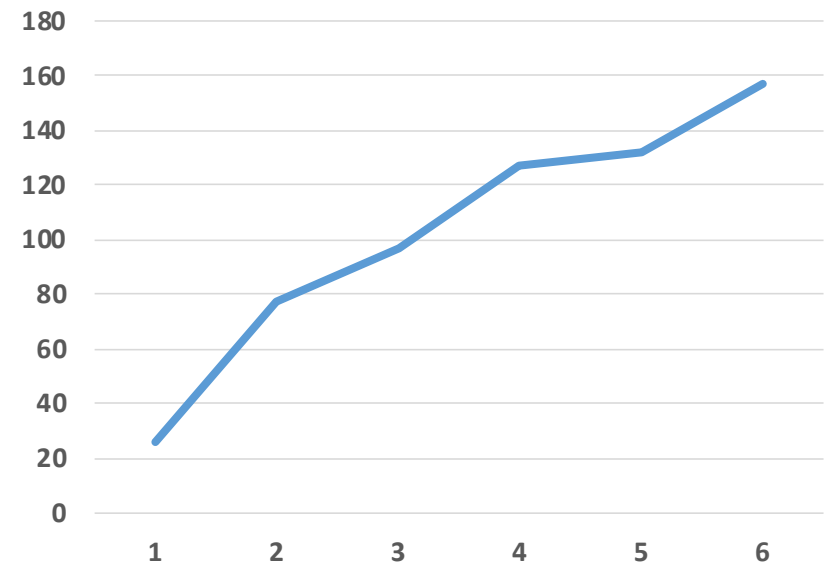
Industry develops CNY exercises

- Provides DIRECT alignment with workforce needs
- Faculty update curriculum 2x year!

Students see path:



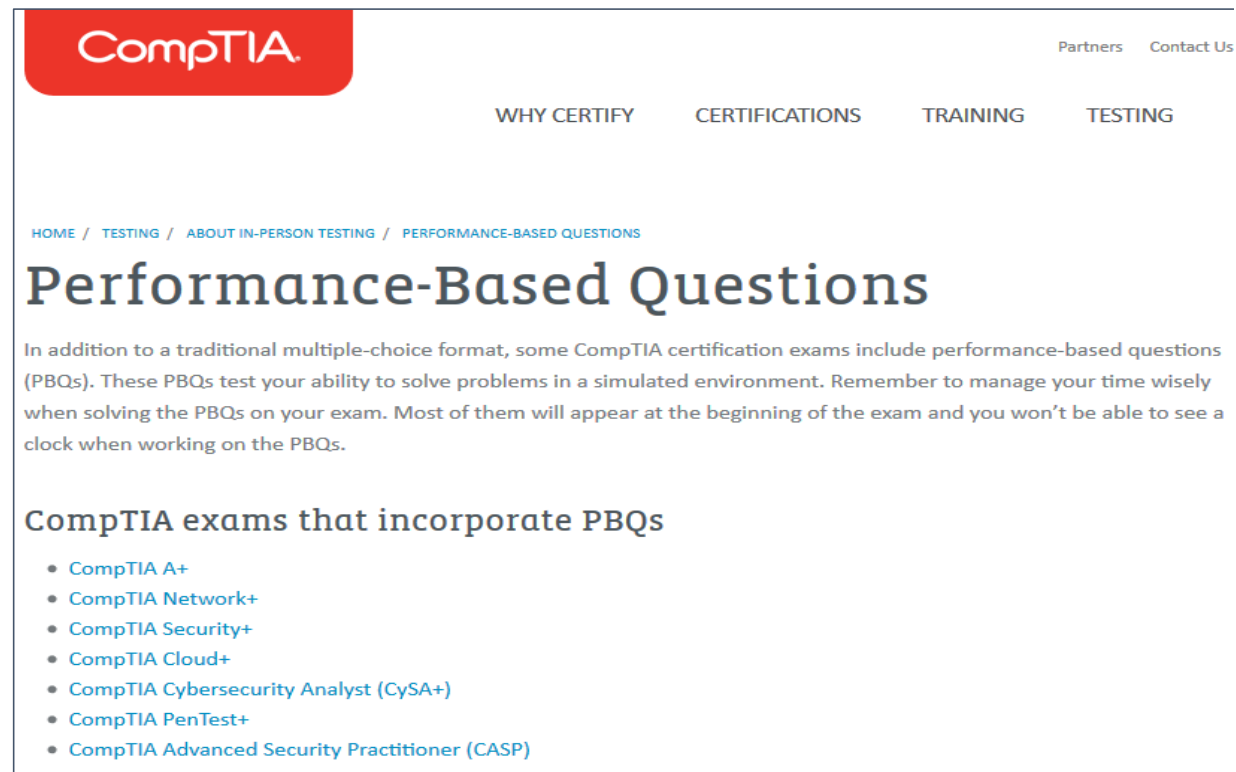
Cybersecurity Enrollment



Benefit to student's next stage of development

Cyber is such an APPLIED discipline — it is uniquely geared toward competency-based education

Competitions map to Security+ and Certified Ethical Hacker “scenarios” later in careers



The screenshot shows the CompTIA website's page for Performance-Based Questions. The page features the CompTIA logo in a red box at the top left. Navigation links for 'Partners' and 'Contact Us' are in the top right. A horizontal menu contains 'WHY CERTIFY', 'CERTIFICATIONS', 'TRAINING', and 'TESTING'. Below this is a breadcrumb trail: 'HOME / TESTING / ABOUT IN-PERSON TESTING / PERFORMANCE-BASED QUESTIONS'. The main heading is 'Performance-Based Questions'. The introductory text explains that some CompTIA exams include performance-based questions (PBQs) in a simulated environment, where time management is crucial. A section titled 'CompTIA exams that incorporate PBQs' lists the following certifications:

- [CompTIA A+](#)
- [CompTIA Network+](#)
- [CompTIA Security+](#)
- [CompTIA Cloud+](#)
- [CompTIA Cybersecurity Analyst \(CySA+\)](#)
- [CompTIA PenTest+](#)
- [CompTIA Advanced Security Practitioner \(CASP\)](#)

Failure at CNY Hackathon?




Failure to work as a team

Failure to learn anything

Failure to be ethical

Success at CNY Hackathon:

Great team comes together OR epic failure leads to lessons learned!



Case Study #3: Practice, training and education for the cyber workforce

National Cyber League

Provides an ongoing virtual training ground for participants to develop, practice, and validate their cybersecurity knowledge and skills

NCL uses next-generation, high-fidelity simulation environments

CRYPTO KAIT

EDUCATOR | INFORMATION SECURITY ASSOCIATE | CRYPTOGRAPHY ENTHUSIAST | OVERLY-ATTACHED PUPPY MOM

HOME · ABOUT · CONTACT · WORKSHOPS · BLOG



NOOBSEC TO CYBER-CHAMPION: HACKING THE NATIONAL CYBER LEAGUE FOR SUCCESS

Blog at cryptokait.wordpress.com

Follow Crypto Kait

- SEARCH

Search ...

- RECENT POSTS

NoobSec to Cyber-Champion: Hacking the National Cyber League for Success

Why I Wrote My First Workshop Proposal

Why I Wrote My First

Crypto Kait's NCL story: every season since 2015



Challenge 01 – Open Source

Answer the following questions about security issues.

1. (25 points) What is the CVE of the original POODLE attack?
2. (25 points) What version of VSFTPD contained the smiley face backdoor?
3. (25 points) What was the first 1.0.1 version of OpenSSL that was NOT vulnerable to heartbleed?
4. (25 points) What was the original RFC number that described Telnet?
5. (25 points) How large (in bytes) was the SQL Slammer worm?
6. (25 points) Samy is my...

Kait's Coaching Tips:

The first thing you should have your students do is to have them define "Open Source Intelligence" (the category name) also known as OSINT. While answers will vary, the underlying message should be that it's data that can be collected from publicly available sources.

After they understand the information out there is publicly available, ask them how they would find out how many cups are in a gallon or how far it is to Mars? Hopefully they will answer that they just "Google it."

"Just Google It" is my publicly proposed alternative title for the OSINT section of NCL. This section is based entirely on security trivia or easily researched skills. Tell them this section should be low stress and is the BEST place to start for the person brand new to InfoSec.

Notes: Sometimes, they make some especially hard OSINT trivia challenges. Make sure your students know that not being able to find the specific answer NCL is looking for does not make them dumb or incapable. Sometimes, things are just meant to be difficult. If you get stuck for too long, just move on.

Kaitlyn Bestenheider encourages women and girls in this male-dominated field and shares her experiences:

"I hope to help students gain the confidence to sign up for their first Capture-the-Flag (CTF) competition.

I think NCL is the best CTF for students to do because it's designed to be accessible for first-time cybersecurity students and still be challenging to prepare them for the workforce."

Nevada Cyber Club (NCC)

NCC-1701 team competed in NCL

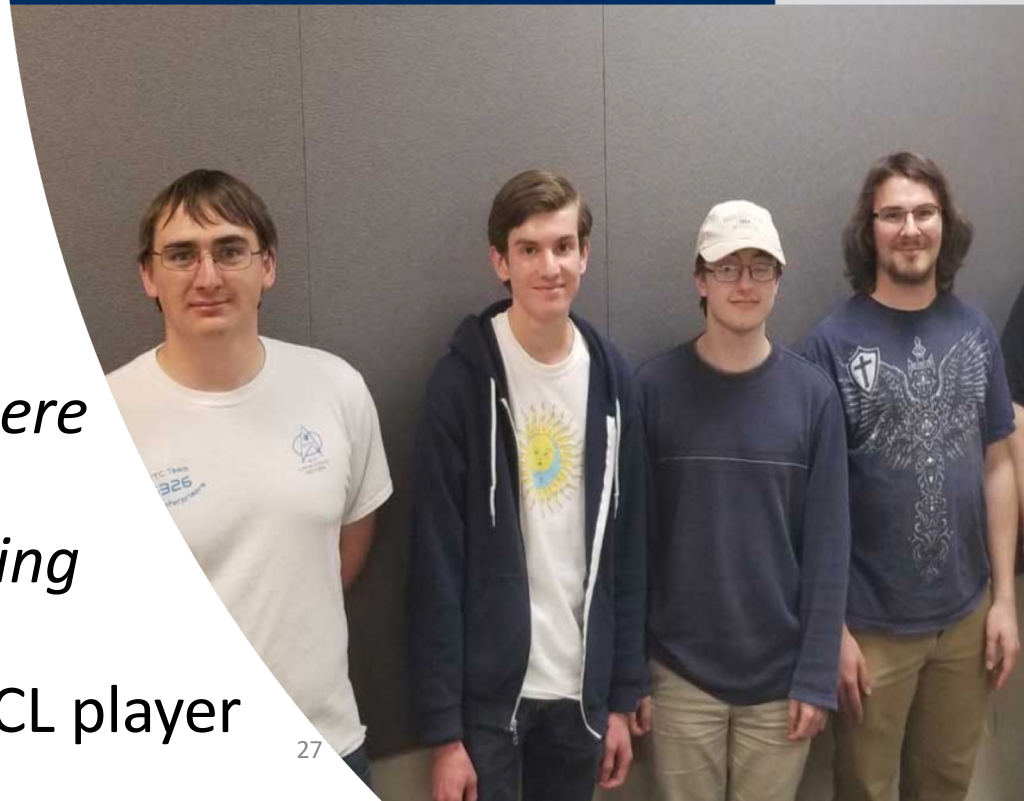
At 3-day national competition, NCC-1701 came in 2nd place out of 264 teams, missing only one of 161 problems

“I enjoy having an environment where I need to be a part of a team with different skill sets to solve challenging and hands-on problems.”

— Alexander Parr, VP NCC team, NCL player

EVADA Today

Cyber Club Scores Big in National Cyber Competition



Paradigm shift needed to address “The Gap”

Growing gap: demand vs. supply of well-qualified cyber professionals

Technical/ virtual environments are important

- Key training for doctors, pilots, emergency professionals, professional athletes

Brain science shows repetition is essential to knowledge retention

- Muscle Memory: repeating tasks over and over enhances neural pathways
- Multiple avenues mean more neural pathways & stronger retention

'Gamification'

Introduces concepts of games into real-world education, training and assessment environments

- Encourages repetition
- Provides positive incentives, not just negative ones
 - >> makes training “sticky”
- As skills improve, challenges should too!

What a good cyber competition can do

- Raise public awareness about cyber competitions
- Exponentially multiply number of cyber games, sponsors and participants
- Inform and restructure academic curricula
- Transform and popularize specific cyber training strategies
- Aid recruiters in identifying talent



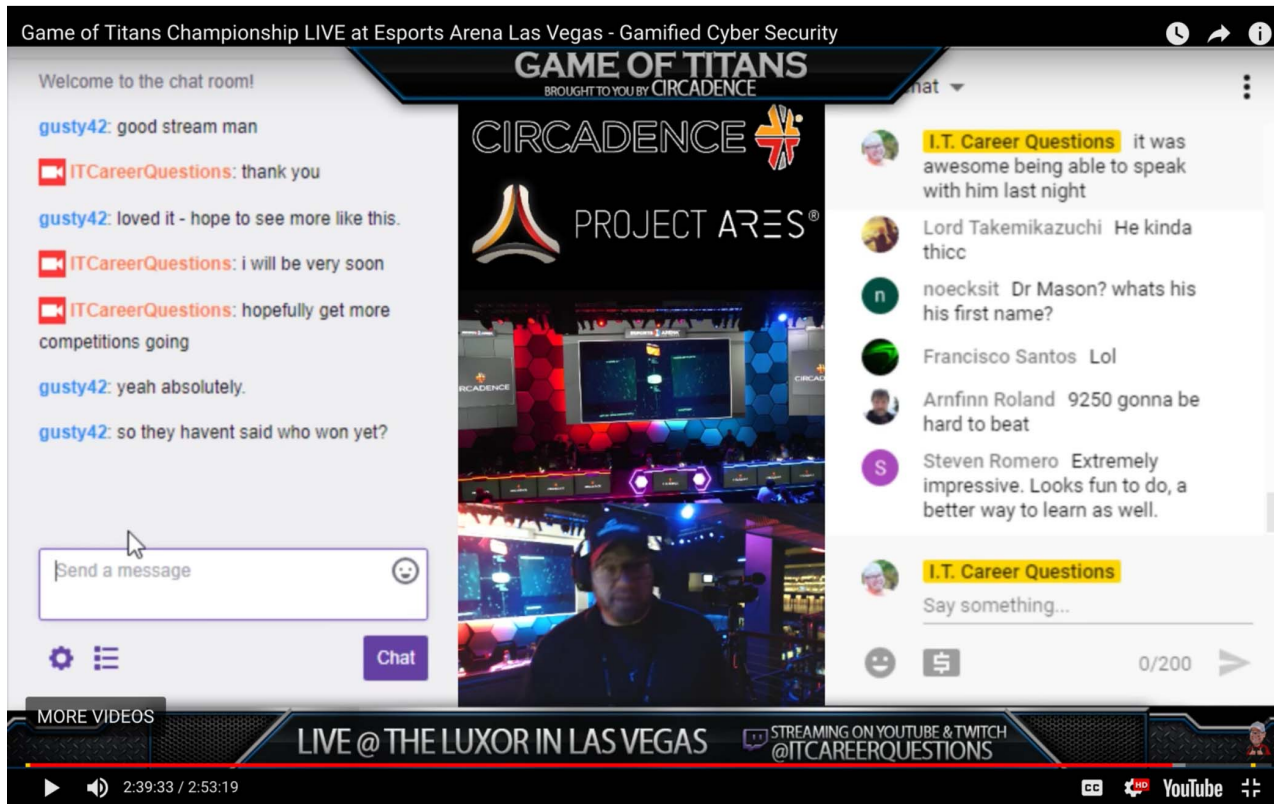
Raise awareness: broadcasting cyber competitions

General public gains understanding & connects personally with cyber

security

Recent global competition in Las Vegas: 2 hour LIVE filmed competition

Congratulations to all winners — including Las Vegas' own Monique Moreno, College of Southern Nevada





Case Study: Advanced, professional cyber competitions



Emerald Down regional exercise

Began at urging from David Matthews – Deputy CISO,
City of Seattle

Pacific North West Economic Region: cyber as an interdependency

First conducted in 2012

- 8 teams live at King County Emergency Operations Center in Renton; other teams in their own locations
- Scenario: Major IT issue, compromised firmware
- IT teams from various organizations



Academia, Government and Industry participated

Various organizations had to cooperate with one another

- Many not used to reaching out
- Learned what other organizations could do

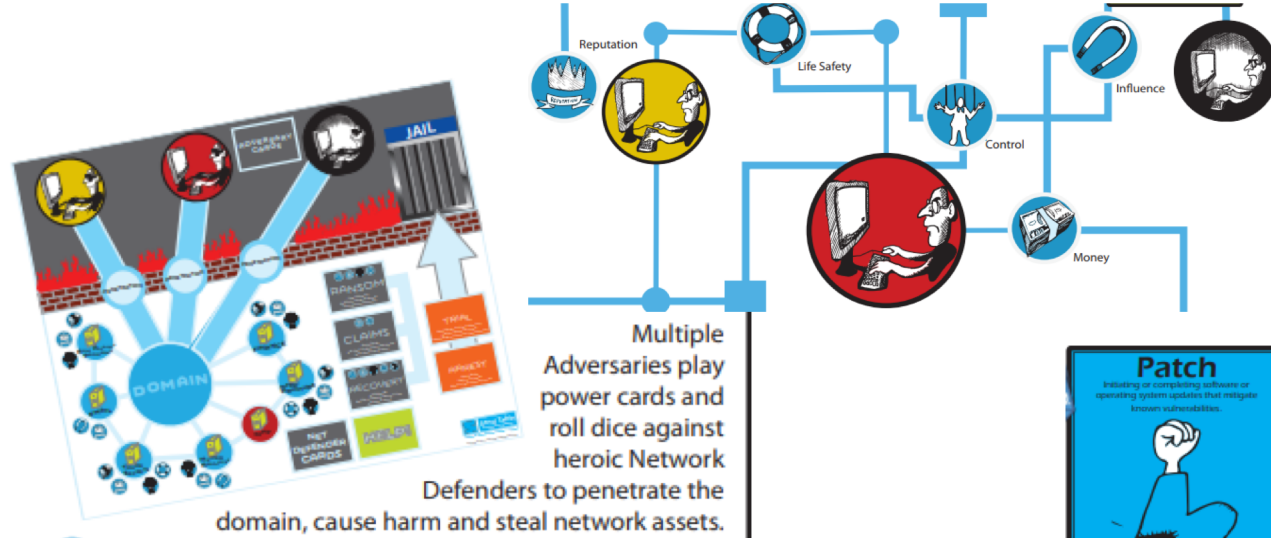
Developed new partnerships and contacts

- Cyber Incident Response Coalition and Analysis Sharing (CIRCAS):
public-private cyber resilience coalition



Emerald Down V: table top exercise

Board game simulated real-life network compromise



Cyber Tactical Resilience Game

Copyright © 2016, James Rollins. All Rights Reserved



Elements of Emerald Down V

- Elements of luck, timing, relative power, etc.
- Game both fun and very enlightening to participants
- Facilitators kept game moving
- Students as Evaluators

Very unique: different levels of government and military had access to varying levels of response

Fascinating to watch:

<https://vimeo.com/207705607>



Extended benefits of advanced exercise

Practiced community cyber security response approach with interactive exercise

Developed Cyber Annex to WA State's Comprehensive Emergency Response Plan
— first in the nation, noted by FEMA & other jurisdictions

Organizations explore how their Cyber Plans could integrate with WA State's Cyber Annex to Emergency Response Plan
Build trust among technology and security practitioners

Failure is the way to success!

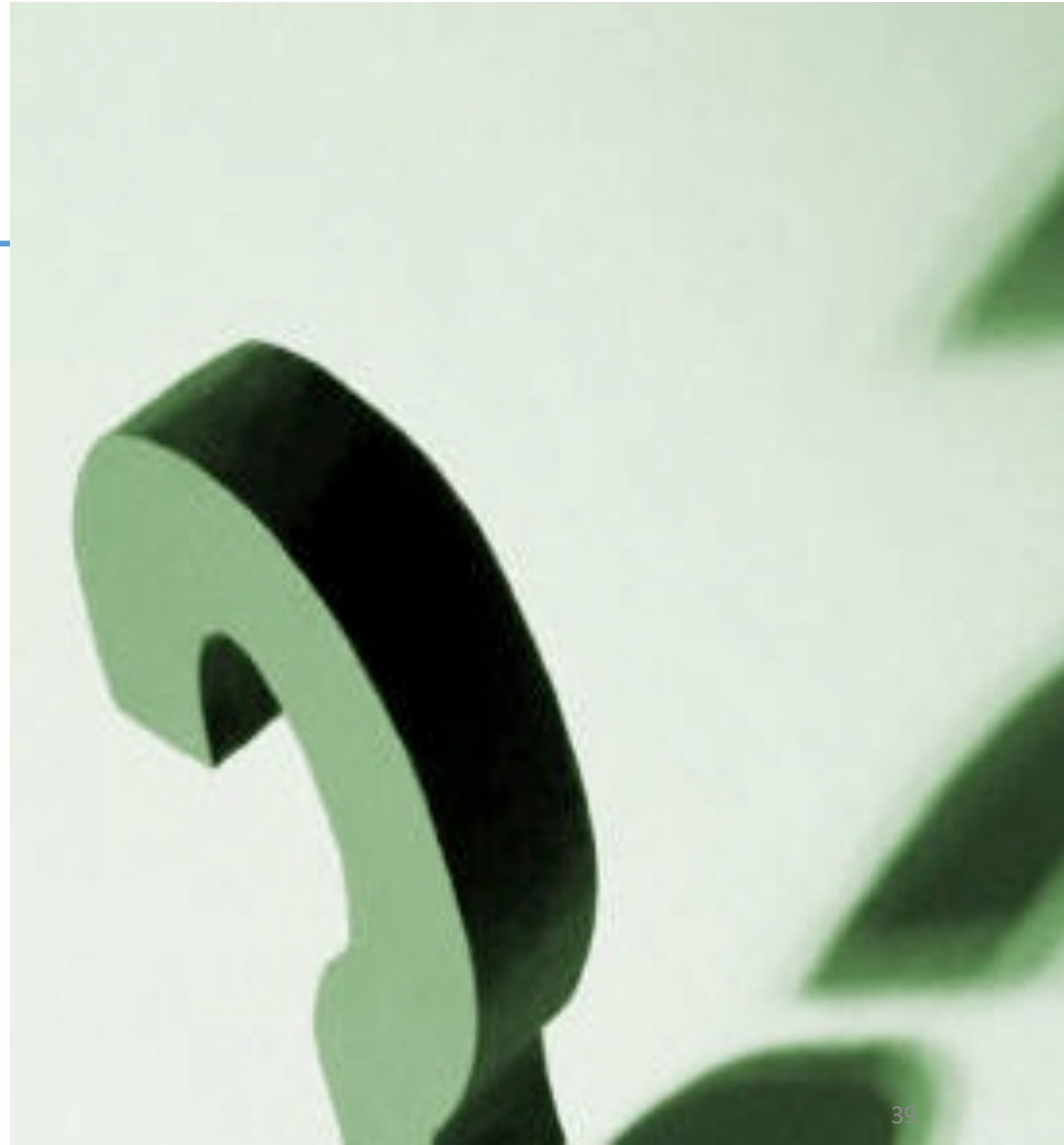
Outcome of exercise is to update the Emergency Management Response plan

Failure identifies where the gaps are

Fix them!



Questions?



Competitions Subgroup deliverables

<https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/competitions-sub-working-group>

One-Pager on Competitions

Cybersecurity Games White Paper

Letter: “Ten Things Parents Need to Know about Competitions”

Links to competition podcasts

Survey on cyber competitions:

<https://www.surveymonkey.com/r/YPXPX8V>

