Tips from Coaches and Mentors of the Year

CyberPatriot Coaching Tips
Mandy Galante - CP-IX Coach of the Year

I have been fortunate to work with mentor Jeremy Milonas, Computer Science teacher extraordinaire and Linux geek. Over the years we have developed these core principles in guiding our teams to success.

Research - teams will get frustrated and struggle because "*I don't know what I don't know*". It's not your job to find the answers, but as a coach you can be constantly on the lookout for new resources. Bring in speakers, look for new online cybersecurity references that the teams can use, find new tools that will improve practice, reach out to the local university that may have their own cyber club with time and expertise to share.

Pave the road - make a commitment to getting your teams the equipment and Internet access needed to compete effectively. Like anything in technology, the minimum requirements to play a CyberPatriot challenge are not realistic. Find out what the recommended specifications are to run all the software associated with CP, especially VMware - then try to get equipped with just a bit more, especially RAM. And since time is a key feature to the competition, adequate Internet access will make a difference! One of our schools couldn't tweak the firewall, so our local borough office allowed the teams to compete on a Sunday from their building.

Promote - spread the word about what your teams have accomplished! Besides making it to Nationals, there are so many other ways for your teams to excel and be recognized. Best new team, first all-girls team, teams that moved from Silver to Platinum, team that made top 10 in States. Let the community know that your teams are rocking CyberPatriot. It will boost player confidence, help with recruiting and inspire support from school administration.

Make friends with IT - many teams practice and compete at school, which offers great advantages. But you will probably have to ask the IT department for some accommodations like a firewall exception or installation of software. Take the time to help IT understand that CP teaches kids to secure systems, not how to hack them. Show them your ethics agreement and explain how the CP students are a great way to spread good cybersecurity practices within the school population. My teams scold their parents, friends and even teachers if they see insecure behavior like a weak password or no updates!

Believe - help the students understand and have faith that the system is fair. In any competition there are some bad apples, but CyberPatriot has a proven record in finding and eliminating teams that don't play by the rules. Direct your teams away from the Internet gossip claims that winning teams are sharing info or that they are handing it down from year to year. When I hear my team members complain of unfairness, my answer is "*I don't want to be standing next to you on stage holding a trophy unless we earned it fair and square.*" Let CyberPatriot worry about what other teams might be doing - tell your teams that hard work, not shortcuts will get them to Nationals.

Look to the future - at its core, CyberPatriot is about opening up opportunities for our students. Being a CyberPatriot can help them get into the right college program, get recruited into great jobs and live cyber smart lives. We found the best way to prove this is to bring back our CP alumni to share their experience post-competition. Last year we set up a "speed dating" format where we brought back 15 alumni, each seated at their own table with 2-3 current students rotating to each table every 5 minutes. The alumni were all at different stages in their life and shared stories about their college studies, how to get an internship, what the job market is really like and, in some cases, how it felt to win a Nationals CyberPatriot trophy!

CP-VIII Coach of the Year
CyberPatriot Coaching Tips
by Allen Stubblefield

1. **New to CyberPatriot**
   a. WELCOME! I took the plunge 7 years ago. Your team's success will depend on YOUR attitude. The first year can be a little intimidating - my email is astubblefield@fjuhsd.org. Let me know how I can help.
   b. **Coach = Facilitator.** You DO NOT have to be the technical expert! Rely on either your students or a mentor to handle that part. Deal with the adults so your students can focus on the fun stuff: competing!
   c. **Year 1 Priorities** (my view):
      i. Getting access to a reliable network.
      ii. Setting up a regular practice schedule. 1-2 times per week is sufficient.
      iii. Understanding how to download, validate and unzip the images.
      iv. For High Schools/All Service - Encourage freshmen and sophomores to join so you can build for the future
      v. For Middle Schools - Encourage 6th and 7th graders to join so you can build for the future
   d. **Recruiting tools:**
      . www.map.norsecorp.com. This represents 1-2% of the actual live cyber attacks. This graphic works at ALL grade levels and is especially effective with school officials.
      i. CyberPatriot official videos.
            1. CP XIII https://youtu.be/XpqWFPnKdSs
            2. CP IX https://youtu.be/sBnONfiV2ck
   e. **Pick 1 Operating System** for your students to focus on
      . Windows - recommended unless you/your students/your mentor have a background in either Linux or CISCO
      i. Linux
      ii. CISCO (not an OS, but a major part of CyberPatriot)
   f. **Team composition:** 4-5 to a team, but I recommend 5 so you have enough on the team to cover multiple systems in the later rounds.
   g. **Training tips**
      . CyberPatriot website
      i. YouTube is your friend
      ii. Mentor

2. **Starting the Year**
   a. Gather interested students and get them excited.
   b. Hold tryouts (even if you are going to keep all of them). Give the students the impression that CyberPatriot is some special. Their attitude and dedication counts.
   c. Establish a regular practice time. My teams practice for 3 hours weekly (1.5 hours x 2 days).

3.   How to approach the Competitions
a.   <u>Use practice and exhibition rounds</u> as a chance to practice like you play.
b.   <u>Emphasize using a checklist</u>. Your students have to put their together so they understand what needs to happen at each point of the checklist.
c.   Insist they <u>use logs</u> to track what they have accomplished. This REALLY comes in handy if they need to restart mid-game and also for the last hour of the game when they are brain dead and need to review what they have already tried.

4.   Putting together teams
a.   <u>Balance</u> - if you have the talent, balance your team(s) so that there are two students covering Windows, two on Linux and one for CISCO/networking.
b.   If you are a new team/cyber program, recommend <u>picking one OS</u> and practice on that this year and go for a 2nd OS next year.
c.   If you are going to have more than one team, don't establish your official CP roster until October in case you have some students who lose motivation or their teamwork skills are lacking.

5.   Determining Success
a.   YOU, the coach, determine success.
b.   Certainly, making it to nationals and winning it all is everyone's goal. However, with an expected 5,000 teams this year for CP IX, picking something more reasonable may help keep your team up for the challenge.
c.   Success can be:
 i.   Scoring better than last year.
 ii.   Scoring better than last round.
 iii.   Scoring better than your other team(s).
 iv.   Scoring better than a local team.
 v.   Finishing your checklist the **1st time through** faster than last round.
 vi.   (you get the picture)

6.   Building for the Future (High School)
a.   Find bright 9th and 10th graders to learn and get better over the next few years.
b.   Host a summer cyber camp and invite middle school/incoming 9th graders
c.   Visit your local junior/middle schools with your 9th and 10th graders. Allow them to sell cyber defense.
d.   Invite the middle/junior school teams to practice with your high school teams.

7.   Personal Lessons
a.   GOOD Mentors are worth gold. We have gone through 3 and currently don't have one.
b.   Students learn best when THEY teach others. Lean on your experienced players to teach others.
c.   The school network is good enough to win on. BUT you need to have the district/school IT personnel's cell phone just in case things go south.

     i.   Network filters may have to be adjusted so that your teams can talk with the scoring engine.

    ii.   Network filters also need to allow your teams to go to anti-virus and anti-malware program websites. Use the practice rounds to make sure that it works.

  iii.   Invite your school IT, principal, district IT, superintendent to come watch a practice or competition round.

    d.   Integrity is a MUST. Teach them what it is, hold them to it and if your students can't be trusted, boot them off of your team.

    e.   Insist that all returning players learn a new area each year. After 3 years, they should be able to handle any computer on the network and CISCO.

    f.   Friday is a tough day to compete - your students have had a long week at school. They need to be FRESH for a 6 hour competition.

Date: September 8, 2015
From: Chris Sutton, Coach Grissom High School
Subject: How to Take your CyberPatriot Teams to the Next Level

I am honored to be chosen as CyberPatriot VII Coach of the Year. The team's Mentors, Chadwick Garber and Frank Sutton, and I would like to share some of the strategies we used to help our team leverage their talents to succeed at the national level.

1. This is our #1: Focus on motivating the students and making it fun. If they enjoy learning about cybersecurity and develop a passion for it, then they'll do all of the hard work of studying and learning what the coaches and mentors teach, as well as researching on their own.

2. Make the team feel special and try to focus on growth and learning, not just winning. We have tremendous support from our Superintendent Dr. Casey Wardynski, and our local administrators. Our teams have their own lab with less-restricted internet access. They enjoy spending time together in "their" space. Also, last year we held a Cyber Homecoming and Cyber Prom with support from Dr. Wardynski, who allowed the firewalls to be loosened so that the students could access Steam for their LAN party. The students were required to dress up and could bring dates. These events helped the students grow socially and strengthen team cohesion.

3. Train the students in the core concepts of operating systems, networks, and services. The CyberPatriot training material is a great place to start. Challenge the students to find the "potential vulnerabilities" as they learn the fundamentals. Ask them to create training images for each other that include the concepts you are studying. However, give them a few boundaries. No live malware. No replacing system commands (yes, I had one student change ls Linux command to shut down the system).

4. Establish and enforce procedures for practices and competitions. Provide a battleplan template which includes each vulnerability category and guide each team to create and continually enhance their own battleplans for each operating system. As they learn new techniques and find potential vulnerabilities, encourage them to update their battleplans. In the spirit of competitiveness and sound ethics, teams should not share their battleplans. This structured approach helps them become professionals. Also, if they use their battleplans in practice, they become fast and efficient with their time. If they jump around and go by memory, they may repeat themselves or miss things. Also, if they have to restart, it is just as important to know which actions were not rewarded with points, to help them quickly recover. Also, help them develop configuration control procedures so they always use the most current versions of their battleplans.

5. Help them to continually expand their base knowledge. This is especially important for the highly competent students who have mastered the fundamentals. Security professionals may have a broad knowledge base, but often specialize in a certain field. Try to bring in several part-time mentors that have depth in various specialty areas: Windows, Linux, Firewalls/Networking, Forensics, Webservers, Databases,

Programming/Shell Scripting, etc. Industry mentors not only provide expertise but help build their confidence. Internships (even unpaid ones) can help the students see how their hard work will pay off in the future.

6. Contact your local professional organizations and request volunteers to come in as guest speakers. Many of these professionals recognize that they will be interacting with their future workforce and want to begin recruiting these individuals to work with them during the summer and after they graduate from college. The organizations that are most active in Northern Alabama are ISSA and ISACA. Also, don't forget local universities and community colleges. Again, this outreach will help them find their future students. If you ask for a guest speaker to come in once, they may enjoy working with your teams and become a Mentor for the season. We keep a core of Mentors, but each season we try to find new Mentors that may be with us for only a season, but can share so much while they are there. If your local resources are limited, try contacting the national chapters of ISSA and ISACA to request a telecom or video conference.

7. As you get further along in the competition, there will be more images than a five-person team can handle. Have the students cross-train with each other. Each team will need more than one expert in each specialty. Make sure your experts are training their wingman/wingwoman. You don't want your team to have a single point of failure. Also, during competition it helps if students can take a break from their image and work on something new. Teamwork is so important and everyone benefits.

8. Encourage teams to develop a unique character and emphasize ethics. Teams should not share information about specific vulnerabilities during or after the competition. This policy ensures that teams are rewarded for their own efforts and that students are expanding their knowledge base, not just piggy-backing on the more experienced teams. Personal integrity and trust are important in the cyber industry which usually requires a security clearance.

9. Practice all year as if you were going to the National Finals. The teams cannot use electronic media during the National Finals, so use only paper notes and don't depend on scripting. Also, have them pay attention to which sites are most helpful so they know which sites they want to whitelist when they qualify for Nationals. Conduct a debriefing after every competition to allow mentors to share their observations with each team independently and help them to improve their battleplans for the next round.

- ## Have students instruct new students as much as possible
    - Teaching others reinforces their learning
    - Even with the beginners, have them teach whatever they have learned to prospective Competitors during open houses; it makes them understand they are getting somewhere

- ## Resources
    - Research on the Internet
    - Cannot rely only on Mentor's knowledge – most are experts in narrow subjects
    - The Coach and the Mentor both need to keep learning all the time
    - Talk to IT people, computer experts, friends – Get ideas from everyone, everywhere

- ## Practices
    - We run two practices each week, often it is much of the same content because there is not one day when all my cadets can practice together
    - Have a plan for what you want to accomplish for practices but be flexible
    - Balance practice vs instruction
    - Repetition, repetition, repetition
    - Train on resetting the images during competition, even experienced teams will lock themselves out or crash images
    - Train on connectivity issues – how to figure out why they are not connected to the internet / network – dhcp, etc.

- ## Competition
    - Read Scenario and Forensic Questions BEFORE doing anything else
    - Plan a restart with 30 - 45 min left, it can take a long time to complete updates
    - Middle School - lots of breaks to keep them engaged mentally
    - Watch what snacks they have when – beware of the sugar crash

- Familiarize yourself with Microsoft Windows tools and resources
  - Microsoft SysInternals Suite Applications that help troubleshoot Windows issues and administer the operating system.
  - Windows God Mode. Windows 7 and 8 feature that allows all Control Panel and Policy functions from one folder on the desktop.
  - Microsoft Baseline Security Analyzer (MBSA) and Security Essentials
  - How to Geek School contains a number of tutorial videos on securing Windows and using SysInternals tools.
  - BleepingComputer Security Tutorials & Tools is another site with information and tools that will help.

- Familiarize yourself with the Ubuntu Linux Operating System
  - The official Ubuntu Desktop Guide is available at https://help.ubuntu.com/12.04/ubuntu-help/index.html. This will help introduce you to the operating system.
  - Fosswire has a couple of cheat sheets. These show commands to run on a terminal / command line.
    - http://www.cheat-sheets.org/saved-copy/fwunixref.pdf
    - http://www.cheat-sheets.org/saved-copy/ubunturef.pdf

- Make sure your team documents everything they do on the images

- Get hands-on practice with virtual images using your MSDN account

- Have students who are not "hands on" the images during competition are taking notes, doing research, and observing the students who are "hands on"

- Have fun!

- Ron's presentation at the October 2014 Online Meeting: http://youtu.be/QmcYUHY8QYI

- Make sure Coaches and Mentors know the students – Don't force learning during unfocused times.
- Find THAT KID to lead and motivate the rest of the team
- Know Coach and Mentor limitations and seek out other resources when necessary.

> – Randy Mills
>   CP-VI Open Division
>   National Finalist Coach

- Have your Mentor know the material better than the students. This frees up the Coach for administrative tasks and provides better support for the team.
- Plan for the competition early and eliminate equipment/connectivity obstacles.
- Recruit students who are motivated self-starters and try to fill out a full team roster.
- Provide supplementary curriculum; the CyberPatriot training materials don't cover everything.

> -- Joe Gombos
>   CP-VI All Service Division
>   National Finalist Coach