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.