# Hack, Play, Win

## Lessons Learned Running the Maryland Cyber Challenge

RICHARD FORNO

Dr. Richard Forno directs the University of Maryland Baltimore County's Graduate Cybersecurity Program, serves as the Assistant Director of UMBC's Center for Cybersecurity, and is a Junior Affiliate Scholar at the Stanford Law School's Center for Internet and Society (CIS). His 20-year career spans the government, military, and private sectors, including helping build a formal cybersecurity program for the US House of Representatives, serving as the first Chief Security Officer for the InterNIC, and co-founding the Maryland Cyber Challenge. Richard was also one of the early researchers on the subject of "information warfare," and he remains a longtime commentator on the influence of Internet technology upon society. rforno@umbc.edu

Cyber competitions are a popular way for cybersecurity practitioners to develop operational skills and acquire and demonstrate abilities and competence in a range of technical and non-technical knowledge areas in the quest for prizes and bragging rights. I describe how the lessons from current competitions can help future competition organizers run successful challenges of their own, and discuss whether such events are sufficient to prepare the next generation of cybersecurity professionals.

An oft-cited and prominent concern facing the Internet security community is the need to identify and hire qualified cybersecurity practitioners able to fill critical technical, analytical, and managerial positions within the global technology workforce. A 2014 report from the Education Advisory Board [1] discusses the "exploding" demand for qualified cybersecurity practitioners, noting that cybersecurity jobs grew by 73% between 2007 and 2012 compared to 6% in all other industry sectors. Similarly, Burning Glass Technologies, a national employment research firm, notes that there are nearly 23,000 available cybersecurity positions in the Washington, DC metropolitan area [2]. Nowhere is this need more evident, or discussed more frequently, than in Maryland, a region some dub the "epicenter of cybersecurity" education, research, and industry [3].

In response to this concern, events in the cybersecurity discipline known as "cyber competitions" or "cyber challenges" seek to motivate and encourage high school and college students toward careers in cybersecurity by developing their technical and teamwork skills while also allowing more experienced cybersecurity professionals an opportunity to practice their expertise in a challenging venue for professional recognition. As a form of intellectual competition, these events are becoming increasingly popular and widespread; industry security conferences like DEFCON CTF or the Department of Defense DC3 Digital Forensics Challenge, and competitions within educational communities such as the National Cyber League (NCL), CyberPatriot, or the Collegiate CyberDefense Competition (CCDC) are but a few examples of prominent cyber challenges drawing worldwide participation. Other competitions, both large and small, continually are under development, as is a National Science Foundation-backed effort to create a national federation [4] to support and standardize the rules, activities, and conduct of cyber competitions.

Given the popularity of these events, and the ongoing global desire to launch new ones, I will draw upon the experiences of organizing and coordinating the Maryland Cyber Challenge in offering advice to current and future cyber competition planners. While no event will ever run perfectly, organizers must always strive to "get it right"—or as close to "right" as possible!

### Event Background

As one of the many cyber competitions emerging in recent years, the Maryland Cyber Challenge (MDC3) is a prominent regional and innovative approach to cybersecurity competitions in support of Maryland's declared leadership in cybersecurity education, research, and industry. However, unlike most cyber competitions, MDC3 is a multi-division event that

simultaneously hosts competitors in high school, college, and professional categories—although teams only compete within their respective division and for separate, quite meaningful, prizes.

The challenge is organized around two virtual qualification rounds leading to an in-person finals event included as an integral part of the annual CyberMaryland Conference held each October in Baltimore. During the qualification rounds (typically spanning a three-day period), teams of up to six players download a specified virtual machine "target" that has been preconfigured with numerous vulnerabilities that must be identifed and fixed within a six-hour scoring window. A similar process is used for the second qualification round, although the target and objectives will change depending on the division—for example, high school teams may face a different operating system, and college/professional teams may encounter a challenge requiring forensics knowledge and the ability to successfully report their findings to the referees for scoring evaluation. Following the qualification rounds, the top eight teams in each division are invited to compete in the finals.

For the finals, high school teams must defend several servers from active attack by an onsite Red Team while simultaneously repairing any vulnerabilities discovered; college and professional teams defend a more complex set of servers while at the same time attempting to "capture"—and then defend—other servers they discover as part of a modified "Capture the Flag" game scenario. To help provide a realistic cybersecurity threat environment for players, the MDC3 gaming platform scores teams based not only on their ability to identify and fix vulnerabilities but also on how well they keep the vulnerability fixed over time. Thus, if a fixed vulnerability is re-exploited later in the day, the team will start losing points until they discover and remedy the situation. Consequently, the scoring process adds to the realistic flavor that the competition provides during gameplay—meaning that teams must embrace a proactive and ongoing cybersecurity posture instead of the commonly held "find-fix-and-forget" mentality found in the operational world. How teams successfully achieve this outcome depends on their ability to coordinate responsibilities, delegate tasks, prioritize actions, and apply other professional "soft skills" within skilled technical operations during gameplay.

Although it is still too early to determine the effectiveness of cybersecurity competitions in providing long-term meaningful value to the cybersecurity workforce, the sheer number of cyber challenges like MDC3 suggests they are considered useful tools in meeting that goal and promoting the cybersecurity discipline more generally.

## Observations and Lessons Learned

Having briefly described the organization of the Maryland Cyber Challenge, I will now reflect on the past four years' competitions to offer readers key observations and insights that may assist in planning, marketing, and running their own cybersecurity competitions.

### *Fostering Gender Diversity*

Perhaps the most striking observation about the Maryland Cyber Challenge is the lack of gender diversity among participants—something unfortunately representative of the cybersecurity profession as well. Meaningfully addressing this situation in both the cybersecurity and broader STEM fields remains an ongoing and prominent concern for schools and employers alike. Much continues to be written and discussed about the ongoing issue of gender equality in computer science [5, 6], but if the educational and professional communities embrace cyber competitions as a way of developing computer security practitioners now, they must also be used to facilitate a more diverse and gender-balanced workforce in the future.

One way to assist in reaching this goal is to ensure that male-dominated clubs and team environments are collegial, tolerant, and foster a culture that does not condone gender discrimination or harassment. Organizations that mentor girls and women interested in cybersecurity or STEM-related fields also play important roles in helping narrow the gender gap in computer science and cybersecurity education. Examples of such groups and programs include the UMBC Center for Women in Technology's (CWIT) "Bits and Bytes" program for high school girls interested in engineering and IT fields and the nonprofit Women's Society of Cyberjutsu (WSC), whose members (current cybersecurity practitioners) regularly teach girls and women about cybersecurity topics and practices via evening seminars, weekend workshops, and summer camps. Although much remains to be done in this area, ultimately each individual must be known, respected, mentored, and utilized appropriately and fairly based upon their talents and capabilities as a member (or potential member) of their desired profession or field.

### *Cheating*

A significant issue facing cyber competition organizers is cheating. For MDC3, this is a concern both during the distributed qualification rounds (conducted unsupervised at a team's own location) and in the finals. To address these concerns, one college team advisor suggested having unaffiliated third-person monitors present during each team's distributed qualification rounds or implementing Web-based video surveillance to monitor the room where the teams were working. In 2014, that same advisor reported that one of his two teams competing in the finals communicated with his other team on technical items regarding the competition. Although initiated with no malicious

intent, the conversation led the first team captain to revisit his own team's work based on information not previously considered. Was this inconsequential conversation akin to intentional cheating through social engineering? When an organization has multiple teams competing, should its teams be prohibited from discussing between them anything about the competition? Given logistical and other resource considerations during distributed qualification rounds found in MDC3 and other competitions, it is likely that such prohibitions are unenforceable, and proposed solutions to monitor teams remotely may not be practicable without significant volunteer, financial, and technical resources. Regarding this particular incident, the team's advisor conducted an internal inquiry and kept MDC3 organizers informed of the situation—ultimately, the team in question was allowed to compete as planned since there was no rule prohibiting teams from the same club at the same university from talking to each other.

During an in-person finals competition event, cheating is even more difficult to ascertain and/or counter: coaches, spectators, teammates, and supporters may develop ways of signaling information to competitors from the sidelines; participants may "bump into" advisors or supporters while going to and from the restroom (if located outside of the competition area); or, in perhaps the most egregious example of cheating witnessed at MDC3, an acquaintance may be positioned outside the competition area with a laptop and mobile phone ready to look up solutions to problems and relay them to the team inside the competition area. Overcoming cheating at in-person events requires not only a degree of trust in the teams and their advisors to abide by the rules, but also active patrolling and monitoring of the area in the immediate vicinity of the competition floor by staff to discover any possible indicators of cheating.

In terms of cheating, although cybersecurity competitions attempt to provide realistic environments for players, they are still only games—and games require a functional gaming environment for the competition to take place within. Therefore, "cheating" at cyber competitions also can include actions taken by participants to attack or disrupt the competition infrastructure (e.g., unplugging routers, DDoS attacks on network connections, and disabling scoring agents or required services on servers) during gameplay to prevent other teams from playing. Minimizing these types of gameplay risks include declaring the game infrastructure itself off limits as part of the competition rules of engagement and deploying network logging capabilities to help facilitate investigation into alleged attempts to "break" the game during play.

Unfortunately, given the nature of the competition, available technology, and potential limitations of facility layouts, it may not be possible to eliminate all sources of cheating during the event. In response to these concerns, although MDC3 never disqualified a team for cheating, it reserved the right to do so under a "one warning and you're out" policy. In such situations, the competition referees (the White Team) would consult with the teams in question, game engineers, and review network log data to determine whether a violation took place. During the first four years of MDC3, there were three warnings issued to teams during the MDC3 finals, but none resulted in disqualification or ejection from the competition.

### *Determining "Student" Standing*

Although many cyber competitions are intended primarily for high school and college students, uneasy situations may arise in establishing what constitutes a "student" vis-à-vis competition objectives. For example, a person may be a highly trained cybersecurity professional at work but also enrolled in a part-time academic program in the evening as a (non-traditional) "student"—however, even though a person is indeed a "student," should he compete in the same division as other "students" with limited or no professional industry experience? In these contexts, other competitors may believe, rightly or wrongly, that some teams are populated with "ringers" who provide an unfair advantage. By contrast, could a motivated high school student compete on a college team in that division, even though she is technically a high school student? To preclude such perceptions or confusion, competition organizers should be mindful of what constitutes a "student" in their event, be flexible in how they approach establishing participant identity and eligibility for the competition, and ensure that these criteria are well-known in advance to all involved. Failing to do that may invite unnecessary drama during the event.

### *Proactive Communications and Outreach*

Perhaps the most important things facilitating a successful cyber competition are the communication and customer service skills of the organizers. Not only is it crucial to set and manage participant expectations appropriately before, during, and after the competition, but when problems in execution inevitably occur, it is essential that teams are informed regularly in an objective and confident manner. Proactive and regular updates to teams (e.g., via email or Twitter) can reassure them that their concerns are noted and that the event organizers are actively working toward a resolution.

For example, in MDC3's inaugural year, a minor earthquake in San Diego created a sinkhole that disrupted communications links to the datacenter containing the MDC3 game environment less than an hour before the start of the first scored qualification round where 35 teams were standing by to compete. By providing regular updates to competitors (including projected estimates regarding repairs and/or when to expect the next situation update), the competition schedule was modified, and despite slipping the exercise start time nearly 48 hours, participants were able to plan accordingly and the competition went forward.

Cyber challenge organizers must never be accused of failing to keep teams informed or being unresponsive to their requests and inquiries—no matter how mundane or inconsequential. Good proactive communication is essential for all types of cyber competitions but is particularly important when dealing with high school students given the typical impulsive nature of adolescent students.

Well ahead of the competition, most organizers publish and/or otherwise inform teams about the rules governing gameplay—and also remind teams of the rules prior to the start of play. However, if any changes are made to the posted rules, they must be promulgated promptly and publicly to all teams. Failing to announce changes to the rules or gaming environment quickly (e.g., "Target #3 is disqualified for all due to unspecified technical problems; no points will be awarded for any work done on Target #3.") may lead to confusion, lost time, or anger exhibited by teams not aware of the change.

### *Avoiding Vulnerability "Conditioning"*

In terms of training and educating students on cybersecurity practices, one of the key characteristics of MDC3 also is one of the most frustrating to participants. Specifically, MDC3 does not disclose what vulnerabilities are present or used for scoring on competitor systems, even after the scores are calculated. For example, if a team only found half of its assigned vulnerabilities during the qualification rounds, frequently they will inquire which vulnerabilities they missed so that they "can learn how to find and fix them" in the future. However, computer security vulnerabilities can manifest in many different ways and yield similar effects; therefore MDC3 organizers do not want to condition teams into believing that a certain vulnerability could only appear as it did during the competition. This policy is revisited regularly by event organizers but as of 2015 remains in place.

### *External Internet Access during Finals*

During the in-person finals, another area of possible controversy regards access to the public Internet during gameplay. For MDC3, although teams were free (and expected) to use the Internet to research vulnerabilities and solutions during the distributed qualification rounds, during the onsite finals teams either had no or extremely limited Internet access (e.g., a shared and paltry 256K bandwidth assigned for the entire competition network) as a way of discouraging participants from using it during gameplay. This was done to reduce distractions such as social media use and to prevent cheating by teams planning to pre-position scripts or other tools on private external servers to gain an unfair advantage.

To compensate, the MDC3 game environment includes an internal patch server that allows teams to download whatever Windows or UNIX updates they believe are necessary to harden their systems and ensure availability. In cases where a team wants a particular tool or patch that is not available (such as a free, open-source tool like nmap), it may initiate a request through the White Team, who in turn discusses the request with the competition referees; if the request is granted, the game engineers will acquire the files in question and place them on the internal update server while the White Team announces to all participants that the new files are available. This ensures that no team has an unfair advantage in terms of software or technical resources. Of course, to help prevent cheating (which may include external access to the Internet), MDC3 maintains a "no mobile device" policy on the competition floor during the finals; however, it allows teams to use paper-based resources such as reference books, notebooks, or printouts they wish to bring to the event.

### *Cyber Challenges as Bragging Rights*

Regardless of student or professional status or amount of prize money won, involvement with and/or winning a cyber competition is considered an attractive activity to list on a resume to demonstrate operational commitment to cybersecurity. Indeed, participation in cyber competitions is an attractive factor when corporate recruiters evaluate students for internships or other entry-level positions. Similarly, professionals competing in such events "on company time" have a strong interest in proving their skills to colleagues and supervisors, often with the strong support of senior leadership: for example, in 2011, the first-place MDC3 professional team was granted entry to the global Cyberlympics finals taking place the following week—their CEO offered strong support and authorized additional travel and time away from the office while they were onstage receiving their MDC3 prize.

As such, competition organizers should be prepared to generate award certificates, participation letters, or other "proof" of a participant's involvement beyond the awarding of any trophies, plaques, or bestowed "bragging rights"—which may include working with local media on stories profiling individual participants, teams, their schools/employers, or their preparations for the competition [7]. To support these efforts, competition organizers should maintain excellent records of scores, scoring criteria, and their interactions with teams that can serve as references if/when questions arise over competition outcomes.

### *"Unknown Unknowns" and the Competitive Spirit*

As with any large event, competitive or otherwise, there will be spontaneous issues, problems, concerns, and situations that organizers did not consider during the planning process. This is particularly problematic when planning cyber competitions for elementary and high school participants, where organizers not only must coordinate competition items across multiple schools, school districts, and states, but may not be aware of every conceivable special situation or resource limitation (i.e., policy,

financial, infrastructure, scheduling, or instructional) facing those schools. As a result, unanticipated incidents may present the event in a less-than-favorable way to school administrators or parents.

For example, during the inaugural MDC3 in 2011, one high school team discovered they could not maintain steady access to the game environment during the first qualification round due to an updated configuration of their school's firewall following the earlier practice rounds. Upon encountering this problem, and unbeknownst to their faculty advisor, the team simply modified their school's firewall and continued competing in the round. While their ingenuity allowed the team to move into the second qualification round, the team's faculty advisor (and computer science teacher) was forced to defend the team's actions to the Principal and school IT Manager the following week—at which point school administrators became aware of the nature of (and skills needed for) such competitions. Although the incident was resolved without punishment, it exemplifies some of the "unknown unknowns" that can arise when highly motivated young participants embrace the competitive spirit. Thus, when preparing for competitions, regardless of student or professional status, teams should ensure that all competitors are cognizant of any local computer use or security policies and coordinate their actions with the appropriate IT staff well in advance of the event. Here again, proactive and ongoing communications with all involved can minimize the potential for confusion or unfavorable views on either the team or competition.

These are some of the more noteworthy observations and recommendations emerging from the first four years of the Maryland Cyber Challenge. Although no organizing team can predict every contingency, appropriate prior planning, proactive communications, diligence in maintaining a fair and diverse competition environment, a degree of objective operational flexibility, and effective management of the expectations of all involved can help facilitate successful and meaningful events.

## Final Thoughts and Admonitions

As a partial retrospective, I have shared some key observations and lessons learned from the first years of the Maryland Cyber Challenge (MDC3) in an attempt to offer useful advice to current and future competition organizers in helping them develop and conduct successful events of their own.

Cyber competitions are a useful tool for the cybersecurity industry. However, in developing the cybersecurity workforce, we must be mindful that cybersecurity competitions tend only to emphasize the demonstration and application of specific hands-on skills to address technical symptoms of current problems versus developing the fundamental or interdisciplinary knowledge to remedy, if not prevent, their root causes [8]. While certainly necessary for success in cyber competitions, and quite useful in the world of technical cybersecurity operations, the knowledge and attributes needed by well-rounded security practitioners—indeed, professionals in any field—must extend beyond the (albeit important) technician-level skills that cyber competitions like MDC3 inculcate. As suggested in a recent Pew research survey [9] and by political observers [10], personal characteristics such as self-reliance, inquisitiveness, critical thinking and analysis, teamwork, strong communication skills, adaptability, excellent organizational or management capabilities, understanding of the theoretical foundations of technology, and situational awareness maintained across an interdisciplinary spectrum are just as, if not more, important as technical skills to a person over the length of their professional career.

Indeed, developing and/or possessing excellent technical skills may qualify a person for a series of jobs that earn a paycheck, fill critical roles in industry, and help meet the politically expedient goal of workforce development—however, a career in cybersecurity involves a far broader set of knowledge, skills, and abilities. Therefore, while cyber competitions are popular events that encourage many toward or further into a career in cybersecurity, we must remember that cybersecurity itself is an interdisciplinary field—and that not all positions in the cybersecurity realm will require expert technical skills honed through competition alone.

***References***

[1] Education Advisory Board, "Multi-Track Cybersecurity Pathways" (Industry Futures Series), Washington, DC, 2014: mirrored at http://www.csee.umbc.edu/~rforno/EAB-Cyber-2014.pdf.

[2] Sarah Halzack, "Report Finds D.C. Area a Hotbed for Cybersecurity Jobs," *Washington Post,* March 8, 2014: retrieved from http://www.washingtonpost.com/business/capitalbusiness/report-finds-dc-area-a-hotbed-for-cybersecurity-jobs/2014/03/08/1b72ff1e-a560-11e3-8466-d34c451760b9_story.html.

[3] Fort Meade Alliance, "Epicenter of Cyber Security": retrieved from http://www.ftmeadealliance.org/mbc/doing-business/epicenter-of-cyber-security.

[4] CyberFed, "About Us," 2015: retrieved from http://cyberfed.org/about.html.

[5] D. Beede, T. Julian, D. Langdon et al., "Women in STEM: A Gender Gap to Innovation," US Department of Commerce Economics and Statistics Administration, 2011: retrieved from http://www.esa.doc.gov/sites/default/files/womeninstemagaptoinnovation8311.pdf.

[6] American Association of University Women (AAUW), "Solving the Equation: The Variables for Women's Success in Engineering and Computing," 2015: retrieved from http://www.aauw.org/research/solving-the-equation/.

[7] Lauren Loricchio, "Catonsville High Cyber Team Members Prepare for the Future," *Baltimore Sun*, October 28, 2014: retrieved from http://www.baltimoresun.com/news/maryland/baltimore-county/catonsville/ph-ca-cyber-security-1022-20141028-story.html.

[8] D. Burley, "An Interview with Gene Spafford on Balancing Breadth and Depth in Cybersecurity Education," *ACM Inroads*, vol. 5, no. 1, pp. 42-46.

[9] Sara Kehaulani Goo, Pew Research Center Blog, "The Skills Americans Say Kids Need to Succeed in Life," February 19, 2015: retrieved from http://www.pewresearch.org/fact-tank/2015/02/19/skills-for-success/.

[10] Fareed Zakaria, "Why America's Obsession with STEM Education Is Dangerous," *Washington Post,* March 26, 2015: retrieved from http://www.washingtonpost.com/opinions/why-stem-wont-make-us-successful/2015/03/26/5f4604f2-d2a5-11e4-ab77-9646eea6a4c7_story.html.