

CYBERSECURITY GAMES: BUILDING TOMORROW'S WORKFORCE





ACKNOWLEDGMENTS


This paper is made possible by the efforts, support and participation of numerous experts and thought leaders on the subject of cybersecurity competitions. It is responsive to the strategic goals of the National Initiative for Cybersecurity Education (NICE) led by the National Institute for Standards and Technology (NIST). The need for this paper was identified by the Competitions subgroup of the NICE Working Group (NICEWG) which has been established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The paper was written and published by the team at Katzcy Consulting.

© Copyright 2016 Katzcy Consulting.

For more information or access to speakers, please contact info@katzcy.com.



Acknowledgments	3
A Note About NIST NICE, its Cybersecurity Workforce Framework, and the NICE Working Group Competitions Subgroup	6
Introduction	7
Competitions: An Overview	10
Why Competitions?	11
The Many Faces of Cyber Competitions	12
Technical Skills vs. Soft Skills	14
Individual vs. Team Skills (and mixed-gender teams)	15
Offense vs. Defense	16
Private vs. Public	17
Short-Term vs. Long-Term Workforce Needs	18
Workforce Development vs. Extracurricular Activity	20
Teachers vs. Students	21
Standardization vs. the Speed of Creativity	23
Tools	23
Scenarios	23
Resources	23
Performance Measurement	23
Taxonomy	24
Fun and Games vs. Means to an End	24
Recommendations	27
Appendices	
Appendix 1: Cyber Competitions Mentioned by Stakeholders	30
Appendix 2: Cyber Competitions List	34
Appendix 3: Contributors	37



Among the diverse opinions offered by this paper's contributors, a consensus emerged: the current and projected workforce needs must be met not only by training more cybersecurity personnel, but also by raising the bar on their skills, aptitude and ability to collaborate. Cybersecurity competitions can play a critical role in this mandate.

A NOTE ABOUT NIST NICE, ITS CYBERSECURITY WORKFORCE FRAMEWORK, AND THE NICE WORKING GROUP COMPETITIONS SUBGROUP

The National Institute for Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce. Its mandate is to promote innovation and industrial competitiveness by advancing measurement science, standards and technology for the enhancement of economic security and quality of life. The National Initiative for Cyber Education (NICE), led by NIST, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure, and provide leadership.

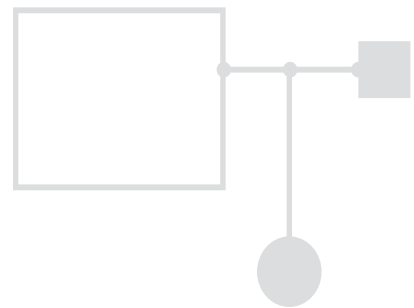
NICE (<http://csrc.nist.gov/nice/nicewg/index.html>) brings together public and private sector participants to develop concepts, design strategies and pursue actions that advance cybersecurity education, training and workforce development. Within the Working Group, subgroups focus on specific topics. The Competitions subgroup is responsible for conceiving this paper and encouraging all contributions.

The NICE Cybersecurity Workforce Framework (a.k.a. the NICE Framework and NIST Special Publication 800-181) provides a blueprint to categorize, organize and describe cybersecurity work into specialty areas and work roles that include specific tasks and knowledge, skills and abilities (KSAs). The CWF provides a common lexicon to discuss cybersecurity positions and roles. It provides a common language to speak about cybersecurity work roles and positions/jobs, and is a reference to help define professional requirements in cybersecurity.

The NICE Framework organizes cybersecurity work into seven high-level task categories:

- Securely Provision
- Analyze
- Operate and Maintain
- Oversee and Govern
- Collect and Operate
- Protect and Defend
- Investigate

As this paper explores themes and priorities for developing cybersecurity skills, the NICE Framework provides a starting-point for creating taxonomy and encouraging standardization that will accelerate growth and expansion.



INTRODUCTION

Whether hacking critical infrastructure like utilities and financial institutions, disrupting political campaigns, stealing intellectual property, or robbing citizens of their identities and sense of security, cyber attackers pose an enormous threat to the American way of life. To defend the nation, its industries and its citizens against existing and emerging threats, the US National Security Strategy is predicated on expanding the skilled workforce to perform duties relating to information security.

A significant shortfall exists between the number of workers with cybersecurity defense skills and the number of open job requisitions, in both private enterprise and government. The federal government faces the greatest challenge with 83% of hiring managers struggling to find and employ qualified candidates.¹ For commercial enterprises, a skilled workforce is imperative; yet experts forecast a demand for 6 million cyber workers by 2019 and a shortfall of 1.5 million.²

To produce this paper, the NIST NICE Subcommittee for Competitions interviewed more than 25 thought leaders from government agencies, defense contractors, other private industry entities and academia. All participants are actively engaged in cybersecurity. They shared their perspectives on this looming issue and the role that cyber competitions might play in raising awareness, enhancing education, attracting capable resources to the field, and addressing the skills gap.³ The interviews sought to understand:

- How **effective are current competitions** at all levels — secondary, university and professional — at developing and demonstrating skills, generating awareness and a pipeline of current and future professionals in the cyber defense field?
- What are the **challenges and opportunities for expanding competitions** beyond current levels to reach larger audiences, generate more skilled resources, and elevate the skill levels of the cyber defenders in the workplace?
- Who might take the **lead in elevating the scope** of competitions across government, academia and private industry?

This paper's stakeholders contributed diverse and sometimes contrasting opinions about the priorities in each of the above areas. The body of this paper details those diverse opinions, addressing such questions as:

- Are technical skills or soft skills more important in producing a strong cyber defense?
- Does skilled cyber defense require individual or group effort?
- Should cyber training and competitions emphasize offense, defense or both?
- Does the responsibility for addressing the workforce shortage and skills gap fall primarily to public agencies or private industry?
- How should investments in education prioritize between short-term and long-term workforce requirements?
- When does standardization of the competition and education process enable scale, and when does it hinder the creativity and agility needed in a rapidly shifting area?

1. http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf, page 28.

2. <http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html>.

3. For the biographies of experts interviewed for this paper, please refer to page 37.

This paper explores whether competitions — as games or as tools for skills development — might be improved through standardization and through an expansion of the competitive arena. The downside of standardization is that it could slow the pace of growth. However, if left to develop at an organic pace, the competitions area — and other aspects of cyber education — may never sufficiently address the intensified needs of the cyber workforce in the short and long term.

Among the diverse opinions expressed, one core belief was shared by virtually every stakeholder: the cyber workforce shortage is so critical that it demands an artificial injection, an impetus, to attract greater interest and participation that will accelerate skills development. The arena of cyber competitions can serve as a significant contributor. Cyber gaming appeals to younger generations, representing both immediate and future cyber workforces. An organized collaboration among key stakeholders can:

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

Cyber competitions, while not alone in these endeavors, are highly effective way of developing skills by providing hands-on experience in simulated, real-world situations. What makes these competitions unique is that the social and gaming aspects of the playing field incentivize participants to be at their most innovative and productive.

When discussing the standardization of cyber competitions, interviewees frequently made comparisons to sports. To the uninitiated, cyber competitions, interviewees frequently made comparisons to their athletic counterparts. There are few cyber stadiums,⁴ few superstar players with recognizable names and faces beyond this specific realm,⁵ no cheerleaders, no endorsement contracts, and no standard rules of the game. Yet, the essence of competition is the same: participants strive to be the best, to excel by recognizing and focusing their talents and to develop winning strategies. Professionalizing cyber competitions can mirror the common structure used by the thousands of sports leagues in the US today. They all rely upon common characteristics for breadth and scale: rules, team roles, organized games, audiences and fans, awards, marketing, and funding through sponsorships and advertisers. The main difference between cyber and athletic competitions underscores the importance of this white paper: a real-world cyber arena exists, where bad actors with malicious intent are inflicting damage upon individuals, corporations and nations.

For **students**, competitions are held at the middle school, high school and collegiate levels and complement classroom teaching and laboratory assignments with hands-on work in a social/gaming environment that fosters learning in entirely different ways. Parents, teachers and other mentors introduce children to the competitions so that students will hone their abilities, learn teamwork, and have fun while exploring avenues for applying their talents in the future.

4. The National Cyber League <http://www.nationalcyberleague.org/> is an example where stadium-like environments have been created.

5. We acknowledge that cyber competition superstars do exist today.

For **cyber professionals** in the private sector, competitions are used to develop and demonstrate skills, to evaluate job candidate abilities, to increase awareness among business leaders, and to boost morale and therefore productivity.

For **industry and certification bodies**, competitions are increasingly seen as relevant work experience for recertification.

For **governments**, competitions are a vital element of generating the skills needed to defend the nation, its industries and its citizens against existing and emerging threats; competitions also strongly complement the other tabletop war games used in training. On the global level, the subject of cyber threats is increasingly the subject of national policy and regulation. Investments are being made to encourage collaboration among all stakeholders to develop and expand the workforce, and to that end, there are a growing number of cyber competitions where nations compete against each other to develop a workforce, and to demonstrate skills and share knowledge (e.g., at the EC-Council's Hacker Halted).

And for **the cybersecurity field** in general, competitions provide an arena to foster innovation: innovation in tactics and techniques, both offensive and defensive, where learning is shared and drives the advancement of processes, technology, knowledge and skills among the competitors.

The opinions, case studies and anecdotes captured for this white paper suggest that cybersecurity competitions are an effective way to raise awareness, develop and demonstrate skills, and deliver an able pool of human resources for recruitment into government or private sector jobs. The social and gaming aspects are seen as particularly compelling for up-and-coming generations of potential workers, and the stakeholders participating in this white paper yearn for cyber competition to achieve what sports leagues have with publicity, followership, sponsorship and participation. They wonder how all aspects of an athletic league, like baseball or football, could be adapted and utilized to both accelerate and broaden the adoption of cyber competitions. This paper makes recommendations on not only continuing but also fast-tracking this discussion, and expanding it to include all interested parties.



COMPETITIONS: AN OVERVIEW

Cyber competitions have been around for over two decades. Mr. Jeff Moss, the founder of DEFCON, created the inaugural event in 1993 to bring together knowledgeable BBS (bulletin board system) hackers to speak, practice and share hacking skills.⁶ Shortly after, this initiative attracted participation from industry and law enforcement in the hopes of developing better cyber defensive tactics and strategies.

Cyber competitions today come in a few different flavors. Many are events where individuals or teams play defense or offense to protect or attack assets in an Internet-connected computer network, or to solve forensic or other cyber-related challenges.

- “Capture the Flag” (CTF) competitions can involve Jeopardy-style questions or hands-on offensive-defensive activity on a network.⁷
 - In a Jeopardy-style CTF, teams are scored and advance by answering questions on topics in various cyber categories including cryptography, steganography, physical security, forensics and scanning.
 - In offensive-defensive CTF, while battling competitors, players endeavor simultaneously or alternately to defend their assets and infiltrate their opponents’ network to assets to reach their objective.
- Operational competitions evaluate teams and award points not only in the technical areas of defending a network and maintaining continual service, but also in business challenges related to an IT security job function (e.g., researching technology or presenting to management). In these types of competitions, a “red team” of expert volunteers perform as hackers, and attempt to break into the network and disrupt service.
- Forensics competitions task students to solve forensic challenges either in a standalone event (see <https://cyberforensicschallenge.com/>) or as part of a larger cyber competition.
- A research paper competition sponsored by the “National Security Agency Science and Security Program” recognizes the best scientific cybersecurity paper from the previous calendar year published in a peer review journal or presented at a conference. Described by Dr. Adam Tagert, director: for four years, this initiative has recognized researchers who have demonstrated lasting impact to the science of cybersecurity. The competition promotes the validity of their research and encourages more quality research in this field.
- Policy cyber competitions, such as the Atlantic Council’s Cyber 9/12 Student Challenge, provide an opportunity for students across academic disciplines to interact and compete to achieve a deeper understanding of the policy challenges associated with cyber crisis and conflict. Using an interactive learning experience with a competitive scenario, exercise teams respond to a realistic, evolving cyber attack and analyze the threat it poses to national, international and private sector interests.

Competitions may be executed in controlled⁸ environments under the supervision of cyber experts from academia, government and private industry who construct the playing field ecosystem, design the scenarios, and usually act as the attackers and role play characters

6. <https://www.youtube.com/watch?v=lg6bQMTjHCE>.

7. <http://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it>.

8. <https://www.govtrack.us/congress/bills/111/hres1244/text>.

during the simulation to best approximate real-world business, government and strategic situations.

Competitions can be conducted entirely online, but the most common type of competition discussed by our stakeholders is a team competition, played in rounds, in live environments where competitors, organizers, judges, educators and sponsors are present. Most competitions score competitors as teams, but a limited few also score individual contributions.

Competitions come from many sources: the brainchild of a single individual or the work of a large, organized group. Their operating budgets are either self-funded or financed by corporate sponsors and government grants. Appendix 2 includes a list of the many competitions discussed by this paper's contributors.

WHY COMPETITIONS?

Sports — participatory contests of strength, skill and speed — have long been used as metaphors for life's contests. Analogies from the sports world are often used to inform everyday discussions on topics from business to education to politics. "Monday morning quarterbacking," "knocked it out of the park," "full court press" and so on — the language of athletic competitions has invaded the lexicon of everyday life in America.

Competition makes for great storytelling. Conflict is universally understood, and tension and interest are created as athletes and spectators eagerly await the outcome of the contests, equally ready to laud the winners and criticize the losers. There's a common desire to prevail and learn from the contests, uncovering the reasons behind a defeat and understanding the strategies that led to a win.

Sports like baseball, soccer and football have taken the competitive structure to new levels.. Youth leagues allow kids to participate in games, learning the fundamental skills, strategies and teamwork required to compete more effectively at higher levels. Competitions held at the middle school, high school and collegiate levels provide further opportunities for individuals to get involved, allowing thousands of young adults to try their hand at these sports and for fans of all ages to engage as they cheer on their hometown favorites. At the pinnacle of these competitive structures is the professional leagues and their championship games. For example, the National Football League's Super Bowl is a sporting event unlike any other. At this culminating moment of the season, the Super Bowl pits two teams of elite athletes against each other, with their heroic exploits broadcast internationally,

"On the playing field, as in the Security Operations Center, skills matter. But trust, communication and teamwork matter more. Cyber sports teach security professionals to think critically and creatively about offense and defense, about the measures and counter-measures associated with every move."

Jessica Gulick, CEO,
KATZCY Consulting

while celebrations are thrown in homes across the country as many Americans gather to watch the game. And sponsors pay premiums.

Cyber competitions generally tap into this tradition of pitting one side against the other. Youth competitions offer participants a chance to learn the fundamentals of cybersecurity in a fun, engaging format and provide an entry point into the professional workforce.

Competitions provide a valuable learning opportunity for participants, regardless of skill level. “Cyber as a sport” is a growing trend in high schools; the number of high school teams that participated in the Air Force Association’s CyberPatriot doubled in a two-year period from over 2,200 in 2014 to over 4,000 in 2016.⁹ Educators increasingly recognize cyber competitions demonstrate and develop planning, leadership, collaboration and communication skills and offer a compelling alternative for students of all ages who are less likely to compete or excel at physical sports.

Finally, the safety, security and enjoyment aspects of competitions should not be overlooked. When practicing both offensive and defensive maneuvers in a typical competition environment, players are encouraged to practice and hone cybersecurity skills in a controlled, real-world environment where no harm can come to the competitors. Moreover, cyber competitions are enjoyed as a forum for networking, team building, and information sharing.

THE MANY FACES OF CYBER COMPETITIONS

In today’s advanced societies, many youth have never experienced a world without computers, cellphones and other Internet-enabled devices. And whether they enjoy Candy Crush Saga or multiplayer games, according to one estimate, the average “21-year-old has spent 10,000 hours gaming — about the same amount of time he’s spent in school from 5th to 12th grade.”¹⁰

Clearly, the social and gaming aspects of competitions are particularly compelling to up-and-coming generations of young people, which qualifies cyber sports as a particularly valuable tool in cyber workforce development. It makes sense to consider how the standardization and professionalization of athletic competitions at all levels have broadened popular appeal, reach and participation. How can a similar approach accelerate the growth of cyber competitions in terms of number, size, reach and stature? However, the stakeholder community is at odds over how best to address the cybersecurity workforce shortage. As cyber competitions grow and evolve around the world in an effort to keep pace with market changes, their relative novelty and expanding adoption create a study of contrasts. The following sections describe key topics where our cyber competition experts held differing opinions on cybersecurity, competitions and the way forward for each.

9. The number of teams registered in 2016 has reached record levels, as reflected in <http://www.uscyberpatriot.org/Documents/CP-IX%20Current%20Registered%20Teams.pdf>.

10. <https://hbr.org/2011/12/millennials-are-playing-with-y>.

LEADERSHIP, TEAMWORK, COMMUNICATION AND CONFIDENCE

Our contributors listed many skills than can be developed through cyber competitions. Leadership, teamwork and communication were most frequently cited. Increased self-confidence was another important benefit.

“The teams who perform well assign roles to team members. One member might focus on firewall and intrusion detection systems. One person might build operating systems and harden them... But frankly, we’re looking for leadership: who is leading, motivating, helping them overcome when they’re ready to quit, because they’ve been hacked.”

Joe Krull, Security Principal Director, Accenture

Communication is essential “to make very compelling arguments as to why certain issues are important, and to determine who can identify consequences, who can make decisions for prioritization and the like.”

Greg Touhill, Deputy Assistant Secretary, Cybersecurity and Communications, Department of Homeland Security (DHS)

Competition builds “self-driven research skills — in these competitions. You’ve got to have the initiative and go out and look for things...find out how to use an exploit to help the team... or run a command. Ultimately, it’s a confidence builder.”

Lisa Jiggetts, CEO, Women’s Society of Cyberjutsu

TECHNICAL SKILLS VS. SOFT SKILLS

Skills development is acknowledged to be a critical outcome for cyber competitors. Many contributors in this white paper cited the importance of teamwork and soft skills as much as they emphasized technical skills improvement. People often assume competitors in today's competitions, and most cyber professionals in the workforce, should be technically trained. Computer science and computer engineering are anecdotally the most desired majors for college students being recruited into the cybersecurity workforce. There are strong viewpoints that cyber competitors and cybersecurity professionals alike must have at least a basic knowledge of "how things work," including networks, threats and malware. This technical emphasis explains the predominant presence of computer science and computer engineering students at cyber competitions, relative to other disciplines.

But the soft skills of leadership, communication (translating technical subjects into business terms), critical/analytic thinking, teamwork, and creativity were frequently identified as desirable characteristics in a cybersecurity role. Several anecdotes from competition observers consistently described team formation, team dynamics, leadership and collaborative problem-solving as characteristics in high demand. Recruiters confirm that these traits lead to job offers being extended to competitors, often during the competitions.

The need for both hard and soft skills in the workforce is well established and extends to the NICE Framework and to certification organizations. As (ISC)²'s Dan Waddell, regional managing director for the North America region, observes "If you put [all certification bodies] in one room and map our certifications to the NICE Framework, it covers the gamut. It covers hard-core technical skills, but also softer leadership/managerial skills, as well. You need a blend."

Although, says Laurin Buchanan, principal investigator at Secure Decisions, "(Competitions remain) focused on high school and college level students, who may or may not be studying computer science and computer engineering — which, from my point of view, is entirely useless to hire someone as a cybersecurity engineer. They don't understand networks; they don't understand threats and malware."

Both technical and soft skills are observable in a competition, as Rodney Petersen, director of NICE, notes: "When I walk around the competitions and observe, I quickly notice the teamwork and how small groups of people are working together. I pick up on non-verbal behavior, leadership skills. From monitoring the activity, you can ascertain someone's technical proficiency, and then their speaking ability, as it comes up in the competition. And employers can do the same thing by walking around and observing them."

Cyber education, of which competitions are a critical part, is often associated with or compared to STEM (or STEAM) education (science, technology, engineering, art and math). Whether this association helps or harms the goal of strengthening and expanding cyber-skills education is unclear. If soft skills are equally as important to a cyber practitioner as technical skills, then a STEM-like approach and STEM-like programs may be insufficient. It has been argued that the present impetus for expanding cyber education is more critical — the defense of our nation, our industries and our citizens — than the concerns that previously sparked an emphasis on STEM education — a declining position in technology skills on the global stage. Therefore, cyber education must be addressed and deployed more rapidly and more widely than STEM.

INDIVIDUAL VS. TEAM SKILLS (AND MIXED-GENDER TEAMS)

There are differing opinions and genuine contradictions about the role of the individual versus the role of the team in the world of cyber competitions and the broader subject of the cyber workforce. Competitions are widely recognized as a source for cyber talent: nurturing future talent in the long term, and proving a hiring source in the now.

While an employee is hired, evaluated and progresses through his or her career as an individual, cybersecurity professionals in the workplace are overwhelmingly expected to contribute as a team. The soft skills associated with teamwork and contributing to a broader business environment are mentioned as frequently as the individual's technical skills.

One of our contributors posited that the white knight or the lone cyber warrior, may be an image conjured up by Hollywood (e.g., as seen, in the television program NCIS). However, other contributors were quick to point out that security training and certification programs focused on the individual could reinforce the notion of being an army of one. In contrast, Mike Cameron, director of business development at Leidos, reminds us, "If you look at the cyber competitions, the ability to succeed is driven not just by individual skills, but how well they communicate as a team to deploy those software skills and team behaviors and function. You're not just training, but you're doing workforce development: you are developing teams as well as people."

With no end in sight to the skills shortage, developing and testing team skills in real-world scenarios appears imperative. Evaluating individual skills and overcoming challenges of scoring (discussed in a later section), stem from the inherent nature of cybersecurity, requiring both individual warriors and well-coordinated teams.

A note on gender and education: one contributor relayed a particularly poignant anecdote about high-school-aged girls who participated in an all-girls robotics competition. Upon completion, the young women were invited to participate in a cyber competition and were asked to choose between a mixed-gender competition and an all-girls competition. One responded that if she had been asked before the robot program, she would have chosen to be on a team with all girls. But now that the team had proven what they could do, they had confidence and would choose to be in a mixed group.

Women are gaining ground in the cyber arena, including in competitions; 2016's Brigham Young University team at the National Collegiate Cyber Defense Competition (NCCDC) notably included four female members.¹¹ Teamwork, the soft skills that come with it, and targeted outreach to girls and women, are all necessary considerations for expanding the cyber competition arena, and workforce.

"There are no lone eagles; this is a team sport."

Greg Touhill, Deputy Assistant Secretary, Cybersecurity and Communications, DHS

11. <http://fortune.com/2016/04/27/mormon-women-cybersecurity/>.

OFFENSE VS. DEFENSE

Whether cyber education and cyber competitions should include offensive skills — the role of the attacker or hacker — is contentious subjects. Most of the contributors who organize and/or sponsor secondary school and collegiate competitions believe that the scope of the game should be limited to defensive capabilities.

In the era of WikiLeaks and state-sponsored hacking, some stakeholders feel it is too much to expect competitions to teach the complex ethical issues of hacking alongside the technical and soft skills required of a cybersecurity practitioner. And there is a lingering bias that practicing offensive skills encourages the wrong talents.

This stance, however, runs counter to the beliefs of some stakeholders who consider the cyber arena to be a battleground. In warfare, understanding offensive techniques is more important than completing technical challenges that merely pit software against software. And as real-world cyber threats become increasingly sophisticated, the need to “get into the enemy’s mind” intensifies. This skill is best developed by walking in the enemy’s shoes and learning offensive methods.

“Playing a part on the blue team in information security can, to a very small degree, be compared to the lot of a hapless soldier. The soldier is told to guard a certain hill and to keep it at all costs. However, he is not told who his enemy may be, what they look like, where they are coming from, or when (or how) they are likely to strike. To ride this analogous horse a bit further, the soldier is given a hand-me-down rifle with only a few rounds of ammunition to fulfill his task. It seems a bit unfair really; even the American Revolution got Paul Revere.”

Verizon’s 2016 Breach Investigations Report

“Being able to look at your defensive position as an attacker, through an attacker’s eyes, is critical,” says Pete Clay, principal of Zeneth Technology Partners. “From my background, a military point of view, my ability to attack has informed my ability to defend. The teams should switch sides; the team that attacks should be on the blue side and defend in the next scenario. The ultimate goal is not just to teach a tactic, which has limited applications in the market. But teaching the tactic and then the defensive techniques to stop bad things from happening, teaching how to orchestrate and use the defenders’ tools to prevent bad things from happen(ing) - this is critical.”

There are pragmatic reasons for allowing competitors to play both sides. Jenn Henley, director of security at Facebook, points out, “If you’ve learned something in a book, by the time you’ve graduated and put it in practice, threat actors and models have changed. Where these competitions are so valuable — they force students to use critical thinking, take foundational skills and put them in practice. It allows them to practice both offensive and defensive [techniques]. Forces them to think as an attacker and a defender. And you can’t get that from a book, or in a classroom.”

PRIVATE VS. PUBLIC

Not surprisingly, during their interviews, many interviewees made an association between patriotism and cybersecurity. In fact, today's cyber competitions draw significant investment and attention from the military services and defense industry. Mike Cameron points out, "The cyber competition community is usually at the nexus of government organizations, academia and professional organizations like the Air Force Association and others."

Public sector funds have helped to jump-start programs, providing seed money to stimulate interest in competitions. The most significant backers of some of the largest competitions, like CyberPatriot and NCCDC, are defense-related organizations or government agencies: the Armed Forces Association, DHS, NSA, Northrop Grumman, and Raytheon, to name just a few.

"Northrup Grumman has taken the lead, put many millions of dollars into Cyber Patriot, even though there is no guarantee that the (participants), will work for Northrup Grumman. (Company leaders) have made a commitment that this is important for our country and our company and our workforce."

Dan Manson, Professor and Department Chair in Computer Information Systems, California State Polytechnic University

Yet, because 95% of US critical infrastructure is in the hands of private industry, it is private industry that has the most to gain in developing a skilled cyber workforce.¹² gain (or lose) in (not) developing..workforce. In competitions that have scaled dramatically, like CyberPatriot and CCDC, most of their funding is private rather than public.

It is widely accepted that private industry faces a real need for highly-skilled cyber employees. To create a labor supply that can meet this demand, most companies will require a business case for investment. That investment strategy may include:

- Sponsoring competitions to increase size and scope, and to expand outreach to students/competitors.
- Providing cyber expertise to competition organizers, helping them develop scenarios, offering staff as coaches and mentors, and staffing the red/white teams, etc.
- Developing technology to enable competitions to scale, working to develop standard taxonomy and process.
- Raising awareness in their communities and among their clientele — and the public in general — about the subject of cybersecurity.

"The US Cyber Challenge focuses on the national level, to elevate the defense of our companies, governments and institutions and citizens and ensure their private and personal information doesn't get into the hands of people who will use it in a malicious way."

Karen Evans,
KE&T Partners, CyberCompEx.org

12. See page 18, section titled "Short-Term vs. Long Term Workforce Needs" for a discussion of the workforce needs.

The private sector typically considers return on investment when making decisions, and a cybersecurity business case will seek to quantify the impact of investing in defensive skills. Business cases usually take into consideration:

- The effectiveness of marketing to increase brand awareness.
- The goodwill generated by associating with the education sector on a topic of critical importance to national defense.
- Investment in and availability of a large pool of highly-trained resources at a fair price point.

This paper's contributors generally believe that scale occurs when the private sector gets involved. New technologies may be developed with government seed-funding, but expansion, adoption and maturity is almost always the result of private investment. In the long run, for cyber competitions, the contributors all agree that the needs and involvement of private industry will ultimately elevate the game to the benefit of private and public enterprises alike. This factor reinforces the importance of ongoing conversations and collaborations among all cybersecurity stakeholders.

SHORT-TERM VS. LONG-TERM WORKFORCE NEEDS

"I tell people; if you want to be a security professional and want to wear a suit and tie every day, there is a place for you. If you want to have purple hair and sit in a corner and not talk to anyone, there's a place for you too."

Jenn Henley, Director of Security,
Facebook

When discussing the role that competitions play in secondary and higher education, and in preparing competitors for careers in cybersecurity, it becomes apparent that there are different needs and expectations in the short term versus the long term.

- Over 1.5 million cybersecurity jobs will be unfilled in the US by 2020.¹³
- A leading Internet-based company reported to the NICE Working Group that thousands of candidates apply for every open software engineering position posted; yet due to the scarcity of skilled personnel, it takes 8-12 months to hire one cybersecurity professional (in an environment with 125 open requisitions).

Re-designing the education system to develop the pipeline for the cybersecurity workforce is a long-term option. The required approach may differ from STEM. STEM is a response to the gradual US decline in the global economy. Cybersecurity skills are needed to face real, current threats of attack on our nation, our citizens and our industries.

13. <http://www.boston.com/jobs/jobs-news/2015/12/08/all-those-scary-hacks-are-creating-a-lot-of-demand-for-certain-computer-experts>.

“I remember when we were doing this for electrical engineers in the 1980s. We had a ‘war for talent’ long before the term was coined. In every case, the demand got met; universities changed their curriculum to educate more people; practical/tactical organizations like SANS began to do it; pay in the field was so much more that people shifted. In every other case, sooner or later, it got met.”

Jim Michaud, Director, CyberTalent Solutions, The SANS Institute

To address the immediate and short-term demand, most agree that other tactics are required. Tactics might include:

- Raising awareness of the need to attract skilled personnel to the field, and not necessarily technically-trained people. As Laurin Buchanan says, “If you’ve found a problem, but you cannot communicate to your manager/CIO/CEO the potential meaning and impact, then having found it will do no good. I find that many technically-skilled people are not very good at communicating in plain language, in simple easy-to-understand terms, what is going on.”
- Expanding professional competitions to develop skills and redeploy resources where they are needed. This opportunity benefits people who are re-entering the workforce or changing careers mid-stream; and based on the statistics cited above, the cybersecurity field represents a “growth industry”, while other traditional job functions are on the decline.
- Creating training programs to address the need at a national level, and consider options for engaging a diverse workforce, including training women and veterans, and offering flexible working conditions. Jim Michaud notes that Alan Paller, president of SANS, makes an analogy between the deficit of InfoSec professionals and the risk to the world and the deficit of pilots before WWII. He points out that, “You do not go to a four-year university in order to learn how to fly an airplane ... you go to a flight school. A lot of SANS courses and competitions are like flight schools. Before WWII, we needed 20 times the number of pilots, and we set up 22 flight schools around the country.”
- Generating interest and enthusiasm among people with the skills, knowledge, or aptitude, to fill cyber positions. To target young people, make cyber “cool” and accessible. For career-age people, increase cyber-awareness and education in ‘mainstream’ courses of study (e.g., top MBA programs). As Jim Michaud comments, “HR professionals have learned from STEM that if we generate interest and awareness early, we can ultimately increase people in the field. In cyber, that’s important, but not enough, and will take too long. Our view is, converting people mid-career from other fields through assessment tools and taking them through our program is important in the short run. Middle schoolers don’t have careers for 10 years, and we need to address the problem NOW.”

WORKFORCE DEVELOPMENT VS. EXTRACURRICULAR ACTIVITY

StackSmash is one example of a professional cyber competition. GE's annual IT security hackathon provides a gateway to cybersecurity at GE. By engaging professionals from IT functions to explore the limits of innovation for real-world security issues, GE has seen tremendous value in imaginative thinking and new tools as well as the by-products of enabling collaboration and building cross-business relationships.

Competitions not only have a place as extracurricular activities for students, but also as workforce development tools for current and advancing professionals. Since much of the interviewee discussion focused on raising awareness in schools of cybersecurity as a subject, a skill set and as a career. This section regarding workforce development is a natural extension of the previous short-term versus long-term debate. Increasing student involvement in cybersecurity is an important long-term strategy, but there are significant short-term needs that must be addressed as well. There is a groundswell of support for professional competitions to enhance the skills of practicing professionals. However, if professional competitions are going to be accepted as tools to train and develop practitioners in the field, then stakes have to be higher than professional bragging rights.

In his iee paper, Dr. Gregory White, Director for Infrastructure Assurance and Security at the University of Texas, references Microsoft's Senior Technology Officer Lewis Shepherd's 2010¹⁴ webcast, *Hiring the Next Generation of Cyber Professionals in Government*. White explains the concern that government agencies, like DHS and NSA, were hiring virtually all the available qualified professionals, leaving private industry to scramble. Foreshadowing today's crisis, Shepherd asked, "How do we train and retrain, and do 'long training,' with our current generation of professionals?"

Competitions can serve to earn certification credits for participants. Certs, like the CISSP and others, require ongoing coursework to maintain their status. Today, credits can be issued manually, but standardizing their issuance should be considered. Businesses can also incorporate competitions into workforce development and standard operating procedures.

As Nasrin Rezai, global CISO of GE Capital explains, "Not only in cyber but in other parts of the company, there are a lot of competition-style ways of promoting new idea generation. Sometimes organizations do it [competitions] one-off, or it isn't a part of their development and workforce planning strategy. We see it as a component of our workforce development. Annually, one business takes the sponsorship; we jointly share cost, and we make it happen. The challenge becomes when you consider it a side job, interest or hobby of the group, instead of a critical component of learning and development."

Another professional development competition is **GhostRed**. This homegrown capture-the-flag competition, has expanded organically within GE over the past five years. What started as a volunteer-driven effort to excite and connect students with hands-on cybersecurity experiences, has now become a formalized GE program designed to recruit top talent into the company.

14. <https://www.youtube.com/watch?v=nwllkcC5KMvA>.

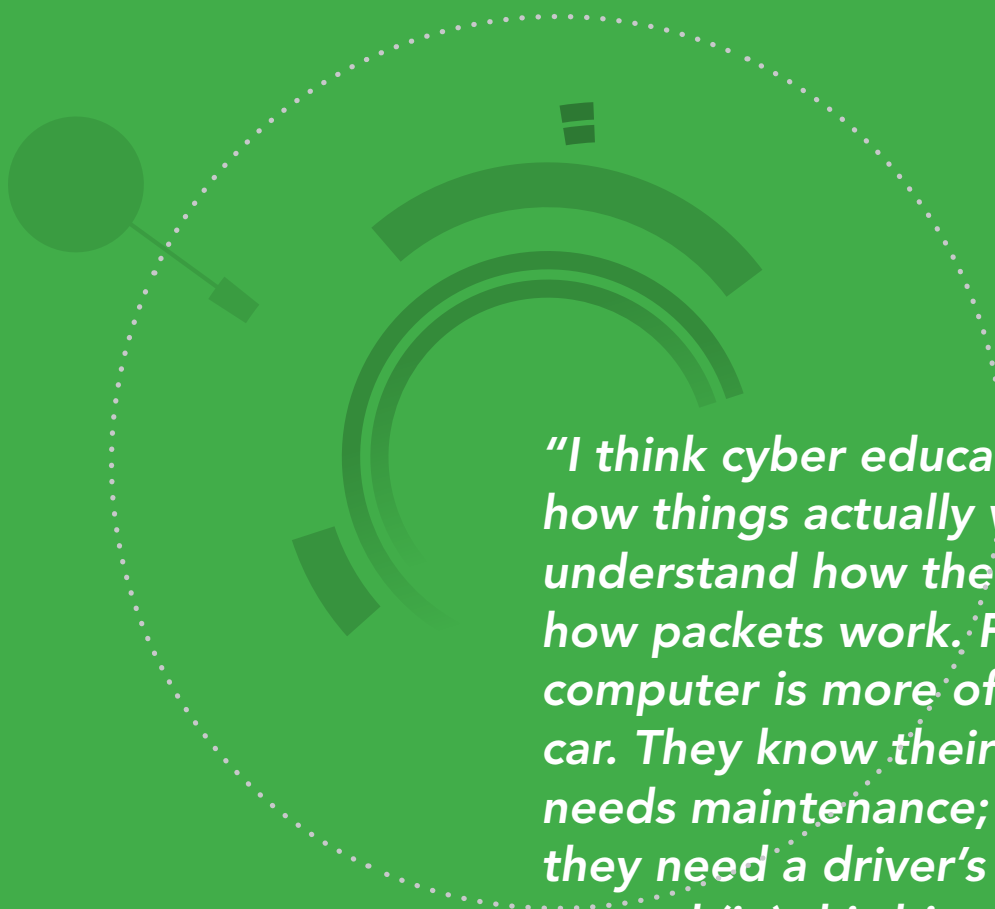
TEACHERS VS. STUDENTS

The interviewees frequently discussed a shortcoming in the education system: students are not generally aware of cybersecurity as a field of study or as a career path. This gap in student awareness is matched by the shortfall in adults — parents and educators — who are aware and skilled to them. Today's first graders are proficient in the use of smart phones and tablets because these devices have been in existence and widely available since their birth. The probability that they know more than their teachers and parents about the use of tablets, because this technology is high.

In this situation, attention is needed to train educators, parents, coaches and the wider education complex on awareness about cybersecurity. In the typical business environment today, senior executives and boards of directors are largely unaware of the threats their companies face, their need to defend them, and how to do so. Education and training is critical at these levels as well.

Changing the education system is not easy to do; many school systems are risk-averse and hold numerous, competing priorities. But if education is about teaching critical skills, Laurin Buchanan suggests "(We must) graduate useful, intelligent members of society and workforce; and we haven't done that with cyber."

Many interviewees made comparisons to their own high school curricula in their analogies to today's need for cybersecurity education: health class and hygiene, physical education, driver's education, home economics and trade/manufacturing-related courses were widely taught, because they were considered critical life skills. These interviewees asserted that the current prevalence of technology and related threats indicates that cybersecurity education can be viewed on equal footing with other subjects taught in schools. Training educators on cybersecurity issues can be made a higher priority; just as driver education instructors are expected to have a driver's license, all educators can be expected to have a general working knowledge of cybersecurity.



"I think cyber education is about teaching how things actually work. You need to understand how the Internet works and how packets work. For many people the computer is more of a black box than their car. They know their car needs gas, that it needs maintenance; there are inspections; they need a driver's license. They can drive around (in) this big, scary thing, because safeguards have already been established.

But the computer, and the amount of damage that can be done to a person's reputation and identity — people don't get it. Cyber education needs to be about explaining how the Internet and networks work; this needs to begin as early as elementary school."

Laurin Buchanan, CISSP, Principal Investigator
Applied Visions, Inc.,
a division of Secure Decisions

STANDARDIZATION VS. THE SPEED OF CREATIVITY

The subject of standardization in the realm of cybersecurity and competitions was not greeted with much enthusiasm by interviewees. In an arena where speed, adaptability and creativity are core defining tenets, there is resistance to adopt standards that may encumber innovation. There is great reluctance to overlay the process of proposing, developing, agreeing upon and adopting standards. But when discussing creating, executing and expanding competitions, several areas were identified where a standard approach would be beneficial to deliver economies of scale in an environment of scarcity.

Areas for standardization and collaboration across competitions include:

Tools

Competitions involve labor intense processes for injecting actions into game play, tracking competitor progress, and scoring individual and team performance. Interviewees recommended automated solutions: Facebook's Capture the Flag platform, Leidos's Cyber NXUS, GE's GhostRed, the Air Force Association's CyberPatriot competition engine, and Secure Decisions' Comic-BEE, a "choose your own adventure story" platform).

Scenarios

Competitions continuously require new scenarios to challenge the participants, especially returning participants. Collaborating on scenario development and developing standard taxonomy were identified to mitigate this challenge.¹⁵

Resources

Effective and challenging events are resource-intensive. Cyber experts develop and run the game, and may participate as red teams. Scaling and expanding competitions must address staffing needs, to consolidate and centralize staff or knowledge.

Performance Measurement

Several interviewees noted the challenge in comparing the scores or results of one competition to another, and more so, comparing the achievements of one competitor to another. This issue was raised most often when discussing the hiring process, and what impression is made when an applicant lists competitions on his or her resume. CyberCompEx.org has taken great strides to map competitive activity to skills within the current field of competitions.

"Everyone gets excited about competitions and wants one of their own; but it's a matter of scaling up with a 'force multiplier' and expanding the reach. There is a cost associated with the competitive platforms and engines. They take time, money and people to develop and update them. If you've ever had to manage the logistics for one of these events, you know what it takes to do it."

Dan Waddell,
Regional Managing Director,
North America Region,
(ISC)², Inc.

15. Bryan Fite, global account CISO for British Telecom, mentions a Scenario Development Language (SDL).

Taxonomy

A dominant theme throughout the interviews was the need to standardize the taxonomy — the roles and definitions — in the cybersecurity workforce, both for competitions and in a professional environment. A human capital perspective was often repeated: establish better-defined team roles that can be commonly understood across organizational and industry boundaries. There were also frequent analogies to sports, with their rulebooks and roles: a football team has a quarterback, defensive linemen, receivers, tackles, as well as a trained, focused and dedicated coaching staff.

“GE actively participates and sponsors numerous high school and college outreach programs to raise awareness and create interest and excitement in technology; and several are focused on girls. After one competition for girls, we asked the participants if they wanted to continue in girls-only programs or go to co-ed programs. They responded: “Before this activity, I would have told you I preferred girls-only teams. But now that I’ve done this and known what I’m doing, I would choose to be in a mixed team.” This response is precisely what GE wants to achieve for the girls: to build their confidence in their knowledge and skills, so that they are comfortable working in technical areas in a mixed group.”

Nasrin Rezai, Global Chief Information Security Officer
GE Capital & GE Digital Security Governance, Tech Risk and M&A

FUN AND GAMES VS. MEANS TO AN END

Among all other objectives, cyber competitions are games intended to be enjoyed by the participants. While interviewees assign a high entertainment value to cyber competitions, a non-expert audience may likely disagree, which is one of the primary barriers when discussing cyber competitions as a competitive sport. The fun comes from meeting the challenge, learning new skills, working on a team, socializing with competitors and sponsors, and achieving success.

Gamification, applying rules, engaging teams, and scoring are widely accepted as effective methods for attracting younger generations (tomorrow’s workforce). But a stronger argument for gamification of the cybersecurity arena might be that those competitive elements — process, teamwork and results — are precisely what it takes to construct an effective cyber workforce.

To set student competitions apart from classroom learning or lab work, it is important to maintain a safe competition environment and remove the pressure of performing that can come with scoring (the equivalent of being graded for classroom learning). Davina Pruitt-Mentle, lead for the NICE’s Academic Engagement at NIST, says competitions “allow students to engage in an informal, non-threatening way, unlike in the classroom where they are graded. If we insist on scoring them, we will turn off some kids, because it takes them out of their comfort zone and away from the idea that they are just going out and having fun.”

And by making the games fun, cyber competitions are viewed by many as a channel for other endeavors: attracting students to STEM fields, and stimulating creative thinking and innovation through intellectual problem-solving. Clearly STEM education is critical to national security, as the *21st Century Science, Technology and Innovation Initiative for America's National Security* report from May 2016 asserts;¹⁶ cyber competitions are compelling method of attracting students to STEM.

However, competitions are not just about education and learning. Nasrin Rezai says, "We think that gaming/cyber competition is a key component of learning, education, and recruiting." Competitions, especially at the collegiate and professional levels, are ideally suited for individual competitors to demonstrate skills and for hiring managers in the government, defense sector and private industry to most effectively identify the best resources with the best skills. There were plentiful anecdotes in the interviews about jobs being offered to competitors at collegiate competitions. In 2009, Boeing, one of the sponsors of the Western Regional Collegiate Cyber Defense Competition (CCDC), hired the entire team from Cal Poly Pomona on the spot. In 2010, one particular competitor was pursued by multiple sponsors on the morning of the final day; they were too late — he was offered a job over breakfast. These examples suggest that competitions might be considered auditions for potential cybersecurity professionals.

Interviews explored whether two concepts — the game itself and a tool for skills development, assessment and recruiting — could be improved by standardizing and expanding the competitive arena. Competitions have been significant growth, with up to 40% increase in participants over the past few years. Over the past few years, participants in competitions have increased by 40%. Is a standardized approach unnecessary? Or does the lack of a trained workforce and the rapid advancement of technology justify intervention?

Consideration has been given to whether competitions can count towards cybersecurity professional certification. Dan Waddell from (ISC)² indicated that currently, a manual calculation process determines whether a candidate's participation and performance in a cyber competition can contribute to the professional development component of maintaining CISSP certification. Expanding competitions, particularly at the professional level, and advancing consistency in their processes and measurement, would facilitate organizations like (ISC)² accepting them as valuable skills development tools and as a part of the certification process. More professionals would participate in competitions improving their skills — to achieve and maintain their certification.

"The Women's Society of Cyberjutsu is committed to providing women professionals with opportunities to develop and enhance their skills in the field. Through competitions, our members learn communication and leadership, along with the technical and system administration foundations that are required. By being a team member, you are both self-driven and on a fast track. It's a confidence builder."

Lisa Jiggets, CEO, Women's Society of Cyberjutsu

16. https://www.whitehouse.gov/sites/default/files/microsites/ostp/NSTC/national_security_s_and_t_strategy.pdf.

17. As cited by Bernie Skoch.

Envisioning the potential reach, structure and impact that cyber competitions might have, several stakeholders rely on the sports league analogies. Sports leagues, for example football leagues, have:

- Standard rule books (with age-appropriate adaptations as needed).
- Defined roles and responsibilities on a team.
- Organized events at multiple levels from Pop Warner to the NFL.
- Booster clubs and leagues.
- Sponsorships and television rights.
- Recognition for teams and individuals, like Heisman Trophies and Super Bowl rings.
- Large, passionate audiences and fans.

These attributes work in concert to elevate awareness of and passion for the sport, and attract athletes to the sport from a very early age. Apart from the love of the game, an athlete's prospect of making a career from the sport is limited. The numbers tell the story: There are approximately 1 million high school football players in the US¹⁸ and under 2,000 players in the NFL.

This is not the case in the cybersecurity arena. With 2 million jobs waiting to be filled, the prospects for young cyber athletes to find employment (after study, practice, and demonstrating his or her abilities) are on the playing field, are great.

Cyber competitions are ideally suited for co-ed play. While female competitors are still in the minority (only seven out of 80 competitors at this year's NCCDC were women), several programs and sponsors are focused on bringing women into the arena. The growing emphasis on the soft skills of leadership and communication is viewed as an opportunity to attract women of all ages, especially women already in the workforce looking to make a career change.

RECOMMENDATIONS

The opinions and narratives of interviewees reflect different approaches and varying priorities regarding:

- Cybersecurity skills development
- Offensive and defensive roles
- Awareness, education and workforce development

The opportunity of competitions—to raise awareness, develop skills, and build a pipeline of cyber professionals — encourage a national dialogue of stakeholders from diverse constituencies:

- Founders and long-standing sponsors of the leading competitions in the US, such as CCDC, CyberPatriot, the US Cyber Challenge, Day-Con, the Atlantic Council Policy Challenge, DEFCON and others.

18. <http://www.cnsnews.com/news/article/terence-p-jeffrey/football-top-sport-us-1088158-high-school-players>.

- Government agencies responsible for developing cyber skills, including the NSA, DHS and the Department of Education.
- Education systems at the federal, state and school district levels.
- Defense contractors who significantly invest in competitions, for skills development and recruiting.
- Private industry, which faces a skills shortage and is well-situated to develop and distribute tools to enable competitions and accelerate product development and differentiation using competitions as a proving ground.

The objectives of this larger dialog should:

- 1** Agree upon areas where collaboration and standardization can facilitate expansion to a larger audience across geographies, age groups, school districts, and public and private enterprises without dampening the creativity and innovation paramount to keeping pace with the attackers.
- 2** Explore how shared investment in technology and process can both compensate for and develop areas of competition that are otherwise limited by resources (people) and sponsors (funding).
- 3** Accelerate the advancement of the following aspects of competitions as well as the cybersecurity workforce as a whole:

“If you impose structure — a taxonomy, an environment — it is much easier to roll out competitions across the USA and beyond. But you also put on handcuffs; what is unique about the cybersecurity industry is that people think differently. This is how they find the unique vulnerabilities in systems. They don’t go after things in a structured manner. A vast majority of cyber experts are self-taught. So we need a structure that can be replicated; but we must ensure there is enough variance to allow ‘out of the box’ thinking.”

Tony Cole, Vice President and Global Government CTO, FireEye, Inc.

Standardizing performance measurement at the individual and team level across competitions

“It’s great that everyone wants more cyber competitions, but without ‘division rules’ it makes it difficult to judge the relative value of one competition versus another. Without knowing whether the A team from one competition is as good as the A team from another, it isn’t an effective hiring guide.”

Bobbie Stempfley, Director of Cyber Strategy Implementation, the MITRE Corporation

“The goals of the NIST NICE Working Group competitions subgroup are in sync with industry: to advance and identify skilled people ready to fill the growing needs of the workforce. The NICE Cybersecurity Workforce Framework is a great place to start to begin to understand the relationships between competitions that develop proficiencies in cybersecurity knowledge skills and abilities and employers who value those knowledge, skills and abilities tie to perform vital tasks in cybersecurity work roles.”

Bill Newhouse, Deputy Director, National Initiative for Cyber Security Education (NICE)

Aligning competitions with the NIST Framework

Developing and sharing competitive platforms

"Until you've done one, you don't know how critical and how difficult it is getting the competition environment working. You need a willing partner, usually a college or university, to host and deliver the resource-intensive tasks of providing working computers, a functional wireless network, enough bandwidth from the ISP, and so on."

Dan Manson, Professor and Department Chair in Computer Information Systems at Cal Poly Pomona./Co-Chair NICE Working Group Competitions SubGroup

"From my military background, I know that my ability to attack informed my ability to defend. You can't only teach defensive tactics that have limited application in the broader marketplace. But teaching attack methods alongside defensive techniques will enable your teams to better prevent bad things from happening."

Pete Clay, Principal, Zeneth Tech Partners

Developing offensive and defensive scenarios

Defining roles and responsibilities within a team of competitors or professionals

"Security is a very broad field ranging from policies, standards and compliance to software engineering and application security. We are now focused on defining and communicating the variety of security roles and how and where they fit into our corporate environment. There isn't a single path into security: there are different skills and techniques and tools to advance a career down a desired path."

Jenn Henley, Director of Security, Facebook

"It's important to understand what is age-appropriate, train the educators, and give them the tools to teach. A good analogy for teaching cybersecurity is teaching health; we teach children about hygiene, bacteria and germs first and then move on to more advanced topics in the higher grades. They need to understand the risk to their personal health and the risk to their cyber health."

Dan Manson, CPP/Co-chair NICE Working Group Competitions subgroup

Training the trainers to enhance educator skills

Raising awareness among students, educators, mentors and parents on the career opportunities for cyber professionals

"Kids don't say 'I want to work in the medical profession when I grow up.' They say 'I want to be a doctor, a nurse, a sonogram technician, an EMT.' They pursue specific roles that they have seen and understand what is involved, that they know who is helped by that person or that role. In the cyber arena today, there is almost no visibility at this level."

Laurin Buchanan, CISSP, Principal Investigator, Applied Visions, Inc., a division of Secure Decisions

"In 1971, there were 700 women and 78,000 men playing high school soccer. Today, 450,000 men and 390,000 women play at that level. For cyber, we want to create a showcase that holds up these mental athletes in as much esteem as physical athletes are held up. More jobs, careers and economic impact will come from this arena than from physical sports, and have(ing) competitive cyber leagues will bring that level of attention, excitement, support and awareness that the field deserves."

Dan Manson, Professor and Department Chair, California State Polytechnic University

Establishing leagues and divisions to support a competitive ladder for varying ages and skill levels

Developing Cyber as a Sport

"Cyber is more than IT. It is our behaviors, actions, and uses — most for good ends, but some for bad. Cyber games train us to know what we're looking for, as well as how best to respond. They develop leadership, communication and teamwork skills in a group of people that typically are more introverted. By developing cyber teams that compete in games like sports teams do, we can establish a code of ethics and a non-military approach centered on collaboration and strategy that will create the workforce we need for the future."

Jessica Gulick, CEO, Katzcy Consulting

Both a great need and a great opportunity exist for all stakeholders in the cyber competitions community to come together to better define the end-goal. Whatever the differences of opinions and priorities, there are significant synergies across all participants; and these synergies can deliver accelerated results through collaboration, coordination and standardization, while acknowledging that creativity and agility must be given a wide berth.



Appendix 1: Cyber Competitions Mentioned by Stakeholders

In the course of over 25 interviews, interviewers described their involvement with and the operation of many competitions at the secondary school, collegiate and professional level. A comprehensive inventory of most competitions is included in a separate appendix; this appendix describes several of the competitions and competition platforms mentioned by the stakeholders.

CyberPatriot for middle school and high school students

CyberPatriot is the National Youth Cyber Education Program. There are three main programs within CyberPatriot: the National Youth Cyber Defense Competition, AFA CyberCamps and the Elementary School Cyber Education Initiative. At the center of CyberPatriot is the National Youth Cyber Defense Competition. The competition puts teams of high school and middle school students in the position of newly hired IT professionals tasked with managing the network of a small company. In the rounds of competition, teams are given a set of virtual images that represent operating systems and are tasked with finding cybersecurity vulnerabilities within the images and hardening the system while maintaining critical services. Teams compete for the top placement within their state and region, and the top teams in the nation earn all-expenses paid trips to Baltimore, MD for the National Finals Competition where they can earn national recognition and scholarship money.

National Collegiate Cyber Defense Competition (NCCDC) for college students

NCCDC's ask competitions ask student teams to assume administrative and protective duties for an existing "commercial" network — typically a small company with 50+ users, 7 to 10 servers, and common Internet services such as a web server, mail server, and e-commerce site. Each team begins the competition with an identical set of hardware and software and is scored on their ability to detect and respond to outside threats, maintain availability of existing services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs. Throughout the competition, an automated scoring engine is used to verify the functionality and availability of each team's services on a periodic basis; and traffic generators continuously feed simulated user traffic into the competition network. A volunteer red team provides the "external threat" all Internet-based services face and allows the teams to match their defensive skills against live opponents.

Day-Con X for professionals

Day-Con is an annual conference dedicated to security training, competitions and information exchange. Started in 2007, the group hosts an annual event in Dayton, Ohio and facilitates Packetwars™ battles, which are described as “Formula One Racing meets World Cup with a dash of Professional Wrestling thrown in for good measure.” Public and private battles provide combatants the opportunity to train and be assessed in a fast-paced and “safe” environment.

DEFCON for professionals

Started in 1993, DEFCON is one of the world’s largest annual hacker conventions held each year in Las Vegas, NV. Attendees include computer security professionals, journalists, lawyers, federal government employees, security researchers, students and hackers with a general interest in software, computer architecture, phone phreaking, hardware modifications, and anything else that can be “hacked.” The event includes speaker tracks as well as social war games and other contents.

Black Hat for professionals

Black Hat is the most technical and relevant global information security event series in the world. For more than 18 years, Black Hat has provided attendees with the very latest in information security research, development, and trends in a strictly vendor-neutral environment. These high-profile global events and Trainings are driven by the needs of the security community, striving to bring together the best minds in the industry. Black Hat inspires professionals at all career levels, encouraging growth and collaboration among academia, world-class researchers, and leaders in the public and private sectors.

From its inception in 1997, Black Hat has grown from a single annual conference in Las Vegas to the most respected information security event series internationally. Today, the Black Hat Briefings and Trainings are held annually in the United States, Europe and Asia, providing a premier venue for elite security researchers and trainers to find their audience.

CyberQuest an online competition qualifier for US Cyber Challenge

CyberQuests are a series of fun but challenging on-line competitions allowing participants to demonstrate their knowledge in a variety of information security realms. Each quest features an artifact for analysis, along with a series of quiz questions. Some quests focus on a potentially vulnerable web server as the artifact, challenging participants to identify its flaws using vulnerability analysis skills. Other quests are focused around forensic analysis, packet capture analysis, and more. The quests have varying levels of difficulty and complexity, with some quests geared toward beginners, while others include more intermediate and ultimately advanced material.

US Cyber Challenge for professionals

The mission of U.S. Cyber Challenge (USCC) is to significantly reduce the shortage in today’s cyber workforce by serving as the premier program to identify, attract, recruit and place the next generation of cybersecurity professionals. USCC’s goal is to find 10,000 of America’s best and brightest to fill the ranks of cybersecurity professionals where their skills can be of the greatest value to the nation.

National Cyber League (NCL) for college students

The NCL was founded in May 2011 to provide an ongoing virtual training ground for collegiate students to develop, practice, and validate their cybersecurity skills using next-generation high-fidelity simulation environments. One of the distinguishing factors of the NCL is the integration of learning objectives in all its activities. One of the main ways this is accomplished is by aligning customized content available in NCL Gymnasiums with simulations and games. This allows players to use the Gym environment to develop knowledge and skills and then demonstrate these newly acquired skills in competitive individual and team play. It also allows the NCL to measure player's game performance and produce individualized reports (NCL Scouting Report) on strengths and weakness among various learning objectives and industry-recognized competencies.

Cyber Defense Exercise (CDX) for the military academies

The Cyber Defense Exercise (CDX) is an annual competition designed to sharpen the skills of our nation's next generation of cyber warriors. The prestigious event, held each spring, tests the ability of students representing U.S. and Canadian military service academies to build, secure, and defend networks from cyber attacks mounted by IA experts.

FireEye's FLARE for students and professionals

Now in its third year, this online challenge has achieved international success. This six-week challenge presents individual competitors with a series of reverse engineering challenges and puzzles targeting engineers, malware analysts and security professionals. Prizes are awarded and online recognition is given.

Cyber 9/12 Challenge for high school students

Now entering its fourth year, the Cyber 9/12 Student Challenge is a one-of-a-kind competition designed to provide students across academic disciplines with a deeper understanding of the policy challenges associated with cyber crisis and conflict. Part interactive learning experience and part competitive scenario exercise, it challenges teams to respond to a realistic, evolving cyberattack and analyze the threat it poses to national, international, and private sector interests. Students have a unique opportunity to interact with expert mentors and high-level cyber professionals while developing valuable skills in policy analysis and presentation. The competition has already engaged over 400 hundred students from universities in the United States, United Kingdom, France, Poland, Switzerland, Hungary, Finland, and Estonia.

CSAW for college students

Cybersecurity Awareness Week (CSAW) is the largest student-run cybersecurity event in the nation, featuring six competitions, an industry conference, workshops and an industry fair. In 2003, it was a small, local competition. Today, CSAW is preparing the nation's brightest students to shape the future of the industry. Every year, it brings undergrad and graduate students together with academic and professional experts to discuss the tools and techniques used by attackers and defenders throughout the field, while students of every academic level (from high school to doctoral) compete in a range of challenges designed to motivate, educate and showcase industry talent.

SANS NetWars for professionals

SANS NetWars is a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world, in-depth skills they need to excel in their field. In SANS award-winning courses, attendees consistently rate our hands-on exercises as the most valuable part of the course. With NetWars, we have really raised the ante, as participants learn in a cyber range while working through various challenge levels, all hands-on, with a focus on mastering the skills information security professionals can use in their jobs every day.

Secure Decision's Comic-BEE for students

Comic-BEE (Comic-Based Education and Evaluation) is a cyber security education technology suitable for all ages and expertise levels, developed with funding from the Department of Homeland Security (DHS) S&T, Cyber Security Division. A scoring capability is being added to enable use of branching, graphic stories as a competition platform, available early 2017.

GE's GhostRed for students

GhostRed is a hands on technology platform for high school and college students to learn cybersecurity. It contains many module and challenges that cover the breadth of topics required to understand the subject matter, from programming, digital forensics, networking many modules and system administration.

Facebook's CTF Open Source platform for students

Facebook began hosting college-level CTF competitions in 2013, and increasingly focused on helping younger kids discover computer science and security. Their CTF platform has been used at dozens of events with organizations all over the world, from the Girl Scouts of America to the University of Cambridge and high schools in Spain. Due to the high cost and technical requirements of building and running CTF environments, few publicly available resources exist for schools, students, and non-profit organizations to use. Additionally, finding any security education resources at the middle and high school level is still a challenge. As a result, Facebook built a free platform for everyone to use that takes care of the backend requirements of running a CTF, including the game map, team registration, and scoring.

Appendix 2: Cyber Competitions List

- 16+
- Middle School
- High School
- 18+
- Collegiate

Competition Name	Level	Location	URL
Cyber Security Challenge UK	16+	United Kingdom	https://cybersecuritychallenge.org.uk/index.php
Cyber Security Awareness Week (CSAW) Qualifications & Finals	High School and Collegiate	US	https://csaw.engineering.nyu.edu
At Large Regional Collegiate Cyber Defense Competition (CDC)	Collegiate	Alaska, Hawaii	http://www.virtualccdc.com/
Collegiate Penetration Testing Competition	Collegiate	US	http://cptc.csec.rit.edu
Digital Forensics Cyber Quest	Collegiate	National	http://digitalforensics.securitytreasurehunt.com/
Information Security Talent Search	Collegiate	United States	http://uscc.cyberquests.org/
Iowa State University Cyber Defense Competition (CDC)	Collegiate	Iowa	https://cdc.iseage.org
Mid-Atlantic Regional Collegiate Cyber Defense Competition (CDC)	Collegiate	Pennsylvania, New Jersey, West Virginia, Maryland, Delaware, Virginia	http://maccdc.org
Midwest Regional Collegiate Cyber Defense Competition (CDC)	Collegiate	Iowa, Missouri, Ohio, Michigan, Indiana, Wisconsin, Minnesota, Illinois	http://www.cssia.org/ccdc/
National Collegiate Cyber Defense Competition (NCCDC)	Collegiate	United States	http://www.nationalccdc.org
National Cyber League	Collegiate	United States	http://www.nationalcyberleague.org/

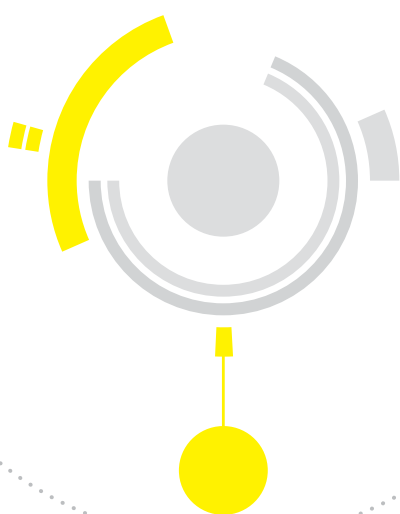
Competition Name	Level	Location	URL
North Central Regional Collegiate Cyber Defense Competition	Collegiate	Montana, North Dakota, South Dakota, Wyoming	http://dakotacon.org http://dakotacon.org/#ccdc
Northeast Regional Collegiate Cyber Defense Competition (CCDC)	Collegiate	Maine, Vermont, New Hampshire, New York, Massachusetts, Rhode Island, Connecticut	http://neccdc.net/wordpress/
Pacific Rim Regional Collegiate Cyber Defense Competition (CCDC)	Collegiate	Washington, Oregon, Idaho	https://www.prccdc.org
Packet Capture Analysis Cyber Quest	Collegiate	National	http://uscc.cyberquests.org/
Panoply	Collegiate	Global	http://www.Cyberpanoply.com
Rocky Mountain Regional Collegiate Cyber Defense Competition (CCDC)	Collegiate	Utah, Colorado, Nebraska, Kansas	http://academic.regis.edu/cias/rmccdc/
Southeast Regional Collegiate Cyber Defense Competition (CCDC)	Collegiate	Alabama, Florida, Georgia, Kentucky, Mississippi, Tennessee, South Carolina, and North Carolina	http://www.seccdc.org/
Southwest Regional Collegiate Cyber Defense Competition (CCDC)	Collegiate	Oklahoma, Arkansas, Louisiana, New Mexico, Texas	http://southwestccdc.org
Western Regional Collegiate Cyber Defense Competition (CCDC)	Collegiate	Arizona, California, Nevada	http://www.wrccdc.org/
CyberPatriot	High School and Middle School	United States	http://www.uscyberpatriot.org
ASIS Capture the Flag	Over 18	Global	https://asis-ctf.ir/home/

Competition Name	Level	Location	URL
Black T-Shirt Cyber Forensics Challenge	Over 18	National	https://cyberforensicschallenge.com
BSides Colombia Capture the Flag	Over 18	Global	Not provided
Codegate	Over 18	Korea	http://www.codegate.org/
Cyberlympics	Over 18	Global	http://www.cyberlympics.org
DEFCON: Backdoor Hiding Contests	Over 18	Nevada	http://www.defcon.org/
DEFCON: Crack Me If You Can	Over 18	Nevada	http://www.defcon.org/
DerbyCon Capture the Flag	Over 18	Global	https://www.derbycon.com
Digital Forensics Security Treasure Hunt	Over 18	Global	http://uscc.cyberquests.org/
Facebook Capture The Flag 2016	Over 18	Global	http://gsec.hitb.org/sg2016/facebook-capture-the-flag/
Ghost in the Shell Code	Over 18	Global	http://ghostintheshellcode.com
Maryland Cyber Challenge & Conference (MDC3)	Over 18	Maryland	http://www.fbcinc.com/e/cybermdconference/default.aspx
NetRiders	Over 18	United States and Canada	http://www.academynetriders.com
NetWars	Over 18	Global	http://www.sans.org/cyber-ranges/netwars
PacketWars	Over 18	Global	http://packetwars.com/
SchmooCon Hack Fortress	Over 18	Global	http://www.shmoocon.org/hack_fortress
Smash the Stack Wargaming Network	Over 18	Global	http://smashthestack.org
UCSB International Capture the Flag	Over 18	Global	http://ictf.cs.ucsb.edu/

List of Cyber Competitions (Provided by Dan Manson)

Appendix 3: Contributors

The views expressed by these contributors do not necessarily reflect the views of their organizations.



Laurin Buchanan
CISSP, Principal Investigator
Applied Visions, Inc., a division of Secure Decisions

A Certified Information Systems Security Professional (CISSP) with over 25 years' experience in Information Technology, Ms. Buchanan has experience both as an information security practitioner and a cyber security researcher. She has a strong technical background in infrastructure, networks and systems, having managed corporate IT operations and security operations, as well as developing information security programs and awareness training at all levels. Ms. Buchanan currently is Principle Investigator for cybersecurity software R&D projects to develop novel techniques for cybersecurity education, cyber security visualizations, and to automatically model and map dependencies between missions, users, and the cyber assets they depend on.

Laurin cut her teeth defending a corporate network from international hackers in 2000, and brought inline Intrusion Prevention Systems onto that network a year later.

She has a strong technical background in infrastructure, networks and systems, having performed and managed IT operations, as well as security operations and architecture. She has developed and delivered security awareness training at all levels. She has created and managed corporate information security programs from the ground up. Coming into IT from business, she understands business needs and compliance concerns and can communicate these to management.

Laurin leads research efforts to develop ways to improve the performance of people who are defending our networks and information, through better education, more usable systems, and leveraging automation wherever possible.



Chris Camacho
Co-Founder and Chief Executive Officer
Ninjajobs

Chris is responsible of the leadership and direction of NinjaJobs. He has over 15 years of technical leadership in cybersecurity and has led initiatives across multiple areas including Incident Response, Forensic Investigations, Security Operations Centers, and Operational Strategy, to ensure Global Financials cyber risk posture are aligned with the business. Chris is an active member of the FS-ISAC Threat Intelligence Committee and serves on multiple cybersecurity and innovation boards.



Mike Cameron
Director of Business Development
Leidos

Mike is the Director of Business Development for Leidos Cyber Operations/AIMO and leads the market strategy and business development for cyber solutions and services across Intelligence, Defense, Civil, and International markets. He is experienced in forming regional marketing and sales agreements with international partners. Mike currently serves as an industry advisor to a NATO working group on Cybersecurity and is a frequent public speaker on the subject of cyber workforce development.



Tony Cole

Vice President and Global Government CTO
FireEye, Inc.

Tony Cole, VP and Global Government CTO at FireEye, assists governments in understanding today's advanced threats and their potential impact. He previously held senior roles at McAfee and Symantec and is retired from the U.S. Army. His last assignment was the Technical Operations Manager for Network Security at the Pentagon and he's been featured in FCW, CNN, BBC, ABC, Washington Times, and many others. He's served on the President's NSTAC IoT subcommittee and was appointed to the FCC's CSRIC-V Council. In 2014 he was awarded 'Industry IT Executive of the Year' by GCN, and in 2015 was inducted into the Wash 100 by Executive Mosaic as one of the most influential Industry Executives impacting Government. He has a BSc in Computer Networking, is the former President of ISSA-DC, and an ICIT Fellow.



Peter Clay

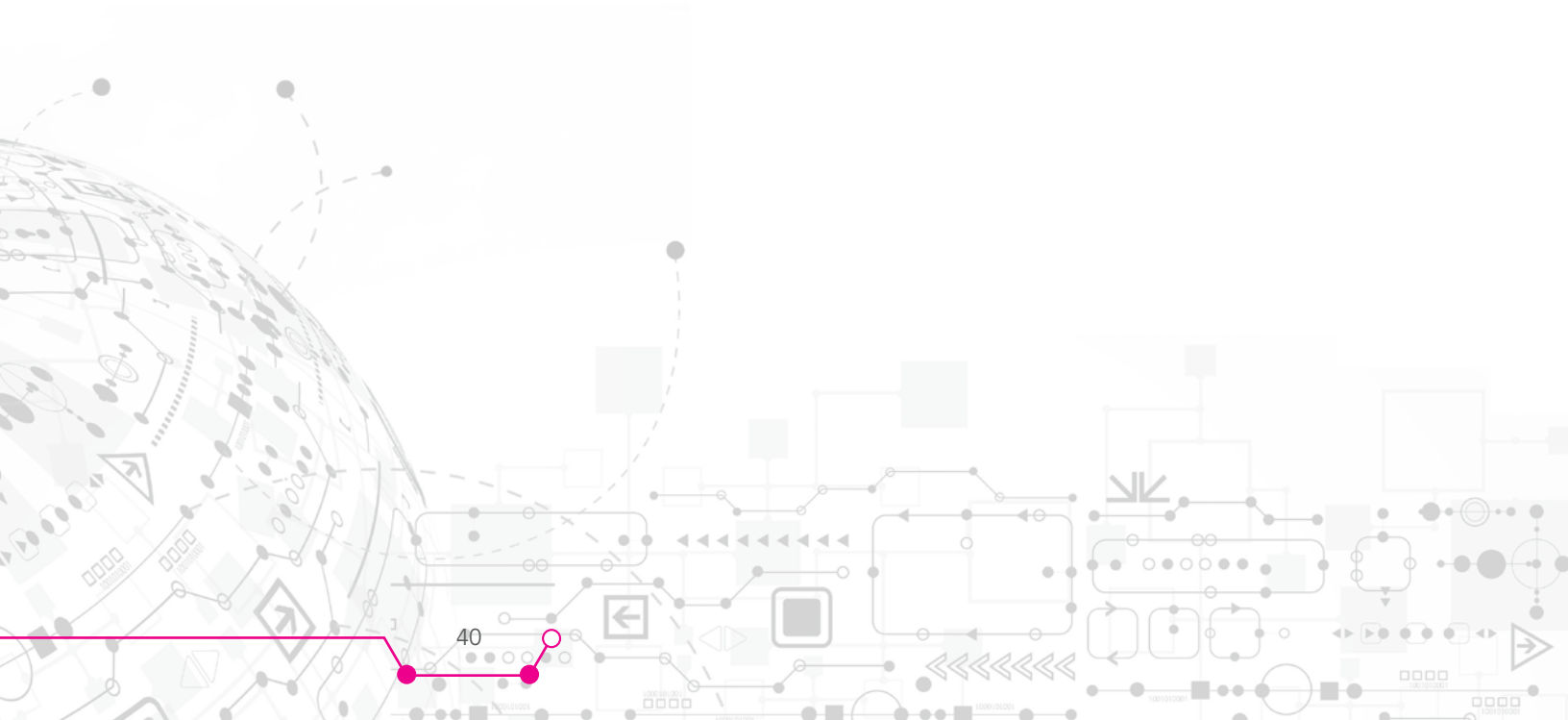
Principal
Zeneth Tech Partners

With over 20 years of experience in Cybersecurity, Peter Clay is a veteran CISO, a visionary practitioner and respected business leader skilled at building highly effective cybersecurity initiatives on a global scale. With notable expertise in making complex security concepts accessible and actionable, Peter embraces innovation, encouraging his teams to think out of the box to achieve risk management objectives. As a Principal at Zeneth Tech Partners, Peter is focused on scaling information security to meet the needs of the other 99% of organizations' information security requirements. Peter is a frequent keynote speaker at industry events and meetings of corporate executive boards and trade associations. He has authored several publications, and been cited as a source for many others. Peter holds a certification in Information System Security (CISSP). An Oxford University-educated historian, Peter brings a unique perspective to cybersecurity, with his passion for American and British history informing his studies of modern cyber warfare.



Karen Evans
Partner
KE&T Partners, LLC
CyberCompEx.org

Currently serving as an independent director and outside manager for publicly traded companies. Karen oversaw the development of over \$70B spent by the federal government in Information Technology and associated services and advised the Director of the Office of Management and Budget on the performance of these investments and the federal enterprise architecture promoting inter and intra-agency cooperation for key Presidential initiatives and cross government solutions. Accomplishments included Homeland Security Presidential Directive 12 regarding authentication; IPv6, Information Sharing Initiatives, Cyber Security, privacy to address the interests of the citizens and government to improve government services through the use of technology and leveraging the federal government buying power and requirements with the establishment of the SmartBUY program. Transparency and accountability were demonstrated with the publication of the Management Watch List and High Risk List, the E-Gov Benefits Report to Congress, FISMA reporting and increased focus on cyber security with the creation of the Federal Desktop Core Configuration.





Bryan Fite
Global Account CISO
British Telecom

A committed security practitioner and entrepreneur, Bryan is currently a Global Account CISO with BT Security. He specializes in using Facilitated Innovation to solve “Wicked Business Problems”. Having spent over 25 years in mission-critical environments, Bryan is uniquely qualified to advise organizations on what works and what doesn’t. Bryan has worked with organizations in every major vertical throughout the world and has established himself as a trusted advisor. “The challenges facing organizations today require a business reasonable approach to managing risk, trust and limited resources, while protecting what matters.”

Professional Highlights:

- Host of Day-Con the annual “Non-Con” Dayton Security Summit
- Founded Meshco™ Producers of PacketWars™
- Introduced Forensix™ computer forensics collection, analysis and visualization suite
- Released AFIRM: Active Forensic Intelligent Response Method to the general public
- Founded GETSecure™ a full service security practice; products, professional services, managed services and training.



Jessica Gulick
CEO and Founder
Katzcy Consulting

Jessica Gulick is founder and CEO of Katzcy Consulting, a woman-owned growth strategy and marketing firm specializing in cybersecurity start-ups and SMBs. A CISSP and PMP, Jessica is a 20-year veteran in the cybersecurity industry with proven experience in strategy, cyber policy, business metrics, global marketing and security program management. She has successfully launched multiple award-winning global cyber marketing campaigns for services, products and cyber competitions. Her portfolio of work also includes the authorship of NIST Special Publications, strategic cybersecurity plans for federal government agencies and white papers for private companies, cybersecurity consulting and engineering projects for national security and financial clients, and a public-private initiative launching the first Maryland Cyber Challenge and Conference. In addition to being a Mach37 mentor, she is president of the Virginia Tech MBA alumni board, vice president of the Society of Women Cyberjutsu national board, and co-chair of the NICE Working Group Competitions subgroup.



Katie Hanson
Director
Sherman Consulting

Sherman Consulting was founded in 1997 when professionals from various industries of organizational development, PR, government and public affairs came together to create a synergy of talents to offer clients strategic and innovative solutions.

As a Director at Sherman Consulting, I offer an entrepreneurial spirit to Sherman Consulting's environment offering innovative solutions for clients in the fields of communications, marketing, public relations, government relations and business strategy, where I oversee various aspects of both strategy and implementation processes. Currently, my focus at Sherman resides in the cybersecurity industry as we facilitate the strategy and advancement of workforce development programs and information sharing that builds the cybersecurity community. We specifically work with organizations and programs including US Cyber Challenge, the Center for Internet Security, the Council on CyberSecurity and CyberCompEx.



Jenn Henley
Director of Security
Facebook

Jennifer (Jenn) Henley is a Director of Security at Facebook. In her role, Jenn is responsible for leadership and planning across the Security organization. On a day to day basis she manages growth & strategic initiatives for the organization and also the team's cross functional relationships with other departments and teams across Facebook. Prior to her employment at Facebook, Jenn was Chief of Staff for the CISO at PayPal. She has over 15 years industry experience, holds her PMP certification and is a graduate of St. Mary's College of California where she received a B.A. in Communications. She also holds an Honorary Doctorate of Humane Letters from Bay Path University.



George Heron
Executive Vice President, Education and Mentorship
Lifejourney

George Heron is the executive vice president for Education and Mentorship at LifeJourney, an online learning platform that enables students to live a day in the life of America's STEM and Cyber leaders. He has a passion for inspiring students to follow paths in STEM education and explore technology careers, and he is active in youth training events, cyber competitions and education-based technology initiatives across the country.



Lisa Jiggetts
Founder & CEO
Women's Society of Cyberjutsu

Lisa Foreman-Jiggetts is the founder and CEO of the Women's Society of Cyberjutsu (WSC); one of the fastest growing nonprofits dedicated to women in cybersecurity. WSC provides women with the resources and support required to enter and advance as a cybersecurity professional. Her organization uses a holistic approach to develop programs that train women in both the hard technical skills and soft skills, leaving them feeling empowered to succeed. She is most proud to be known as a straight-up, but down-to-earth motivator with the women whom she mentors. A service-disabled veteran, she began her cyber career in the military where she excelled as an IT security specialist. Not just a full time geek with a passion for making a difference, she is also an accomplished artist.



Peder J. Jungck

Vice President, Chief Technology Officer
BAE Systems, Intelligence & Security

Peder is Vice President and Chief Technology Officer of BAE Systems Intelligence & Security (I&S) sector. BAE Systems Intelligence & Security enables the U.S. government to transform data into intelligence and provides engineering, integration and sustainment support for critical military platforms and systems. I&S provides services and products to the Department of Defense, the intelligence community, federal law enforcement officials troops deployed around the world.

Peder joined BAE Systems in April 2013 after serving in several key technology leadership positions for Science Applications International Corporation (now Leidos), most recently as the Senior Vice President and Chief Technology Officer of the Cyber Security Group within the National Security Sector. He was also named a Technical Fellow during his tenure. He joined SAIC via the acquisition of the Silicon Valley based CloudShield Technologies, Inc. which he founded in 2000 delivering trusted platforms for cyber security to the defense, intelligence and commercial telecommunications provider communities. Previous roles include leading large scale IT deployments in the retail sector while working for AT&T/NCR, as well as a breadth of IT and Software, CTO and CIO roles for private, public and venture backed corporations.

He has earned 24 patents, published many peer-reviewed papers, a regular conference speaker and co author of the packetC language for cyber and software defined networking. Among his board and advisory board seats, he serves on the board of IT-ISAC on behalf of BAE Systems as well as on the Dean's Leadership Council for Clarkson University's College of Engineering. Peder attended Clarkson University for electrical and computer engineering and received a Bachelor of Arts degree from Beloit College in mathematics and computer science.



Joseph Krull
Security Principal Director
Accenture

Joe provides high-impact professional services to Fortune 500/Global 1000 companies and emerging technology companies. He is an author and frequent public speaker on security and privacy subjects including application security, mobile device security, secure e-commerce, identity fraud prevention, wireless threats and the maturing science of Network Intrusion Prevention. He is a Certified Protection Professional (CPP), Certified Information Systems Security Professional (CISSP), National Security Agency IAM Certified, Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC) and Certified Information Privacy Professional (CIPP). Joe is an Advisory Board member of the National Collegiate Cyber Defense Competition (NCCDC) and a member of the Texas Chief Information Security Officer (CISO) Council.



Marcelle Lee
Adjunct Professor
Anne Arundel Community College,
University of Maryland

Marcelle Lee is a malware analyst, an adjunct professor at Anne Arundel Community College and University of Maryland, and co-founder of Fractal Security Group, LLC. She is involved with several industry organizations, working groups, and boards, including the Women's Society of Cyberjutsu and the ISSA Women in Security Special Interest Group.

Marcelle has earned the CSX-P, GCFA, GCIA, GCIH, GPEN, GISF, GCCC, CIEH, CCNA, Security+, Network+, and ACE industry certifications. She holds several degrees and is currently pursuing a Master's degree in cybersecurity at UMBC. She is a cybersecurity competition enthusiast and an active volunteer in outreach to students and the community.



William Leigher

Government Cyber Solutions Director
Raytheon

Bill is a career U.S. Navy officer with thirty-three years' experience in operations and staff experience in Signals Intelligence, Information Operations, Communications and Network Operations. He has extensive and hands-on experience operating and securing enterprise networks on a worldwide scale. Developed and implemented methodologies for predictive analysis of network intrusion events. Bill is an effective communicator of strategic and technical concepts and plans.



Dr. Daniel Manson

Professor and Department Chair
California State Polytechnic University

Dr. Dan Manson, CISSP, is a Professor and Department Chair in Computer Information Systems at California State Polytechnic University, Pomona (Cal Poly Pomona). Dr. Manson has taught Information Systems Auditing, Internet Security and Computer Forensics in the College of Business Administration Computer Information Systems undergraduate and Master of Science in Information Systems Auditing programs. From September 2003 to March 2004 and January to December 2006, Dr. Manson served as the campus Information Security Officer for Cal Poly Pomona.

Dr. Manson led the effort for Cal Poly Pomona to be designated a National Center of Academic Excellence in Information Assurance Education in 2005 and again in 2008. Dr. Manson is in charge of the Western Regional Collegiate Cyber Defense Competition and California Cyber Challenge as part of the United States Cyber Challenge.

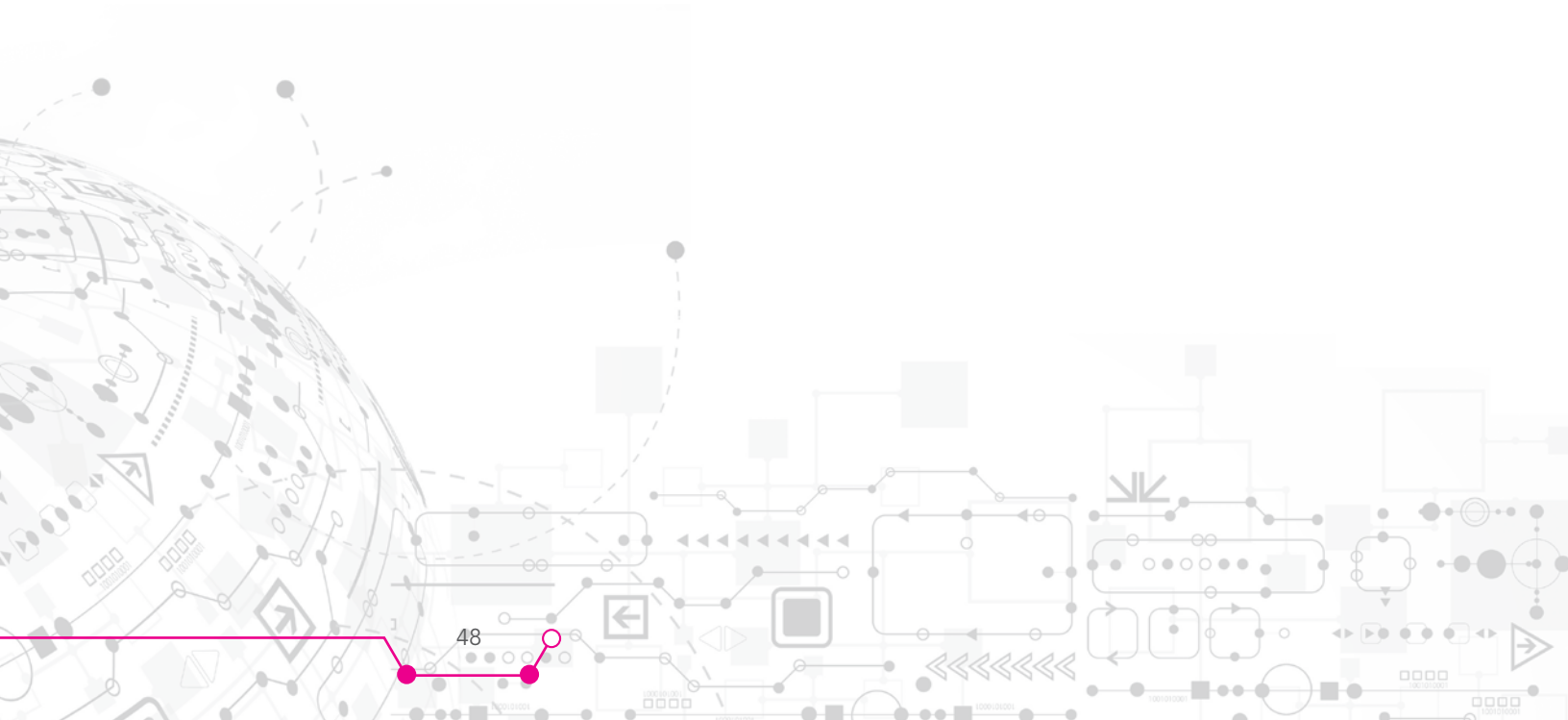
Dan has been co-Principal Investigator on three National Science Foundation grants to support workforce, curriculum and professional development in cyber security, including the current CyberWatch West NSF ATE Regional Center grant. Dan serves on the Academic Relations Committee for the Los Angeles Chapter of the Information Systems Audit and Control Association and is a past president of the Southern California High Technology Crime Investigation Association.

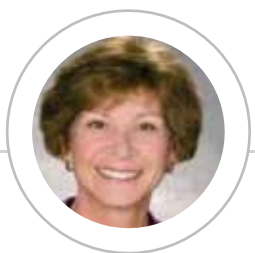


Jim Michaud

Director, CyberTalent Solutions
The SANS Institute

Jim Michaud is the Director of CyberTalent Solutions for the SANS Institute, which helps clients find, develop, and retain qualified cybersecurity professionals. SANS VetSuccess and Women’s Academy programs are bringing new and diverse talent to this critical field. He also teaches human resources at the highly regarded School of Human Resources and Labor Relations at Michigan State University. He is a frequent guest speaker on topics of high interest to the global HR community. Prior to SANS, Jim held senior executive positions in HR at Cliffs Natural Resources, Arcelor Mittal, and Alcoa. He is a Board member of the Detroit Manufacturing Renaissance Council, the Global Employment Institute, and the Michigan State University School of Human Resources Advisory Board.





Diane Miller
Director, InfoSec Operations and Cyber Initiatives
Northrop Grumman Corporation

Diane Miller is the director of InfoSec Operations and Identity Management for Northrop Grumman Corporation, and is Northrop Grumman director of Global Cyber Education and Workforce Development Programs. In her role as director, Infosec Operations and Identity Management, Ms. Miller ensures effective operational leadership of the Information Security function for Northrop Grumman's Global Network and leads all aspects of both assured identity and identity provisioning for the company. In her role as director for Global Cyber Education and Workforce Development Programs, Ms. Miller is the focal point for the corporation's global cybersecurity education, outreach and workforce development efforts, leading its commitment to cultivate a highly-trained, global cyber workforce of tomorrow.

Ms. Miller is a member of the Advisory Board for the IEEE Software Technology Conference, a member of the Association of Information Technology Professionals, and a founding member of the National Software Council. For 12 years, she served on the Editorial Board of the Northrop Grumman Corporation Technology Review Journal. She is a member of the President's Strategy Development Council for California State Polytechnic University, Pomona, the National Visiting Committee for the National Science Foundation's National CyberWatch Center and CyberWatch West, and a member of the Education and Workforce Development Working Group at Department of Homeland Security.

Ms. Miller graduated Magna Cum Laude with a bachelor of science degree in information systems from California State Polytechnic University, Pomona. She is a Certified Computing Professional (CCP), conferred by the Institute for the Certification of Computer Professionals, and is a Certified Six Sigma Green Belt.



William Newhouse
Deputy Director
National Initiative for Cybersecurity Education (NICE)

Bill Newhouse is the Deputy Director of the National Initiative for Cybersecurity Education (NICE), and Senior Security Engineer at that National Cybersecurity Center of Excellence (NCCoE). Both NICE and the NCCoE are part of the Applied Cybersecurity Division in the Information Technology Laboratory at the National Institute of Standards and Technology (NIST).

As the deputy director of NICE, he leads and promotes efforts within government and with those involved in cybersecurity competitions to foster, energize, and promote a robust network and an integrated ecosystem of cybersecurity education, training, and workforce development that can more effectively secure cyberspace.

At the NCCoE, he is leading the drafting of building blocks that address broad technology gaps in cybersecurity implementations that affect multiple sectors. These projects rely on insight and passion from members of various industries who share a common goal of meeting a particular cybersecurity need and will demonstrate commercially available technologies that provide cybersecurity improvements to the multiple sectors addressed.

Additionally, Mr. Newhouse promotes cybersecurity R&D efforts as a co-chair of a Federal cybersecurity interagency working group and as a regular representative to other federal cybersecurity R&D working groups.

Before coming to NIST in 2010, Bill spent five years in the Office of the Secretary of Defense where he worked initially with the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) and then with the Office of the Chief Information Officer for Identity and Information Assurance focused on cybersecurity R&D and technology discovery. Bill utilized the Defense Venture Catalyst Initiative (DeVenCI) to focus on innovative companies working in areas that had the potential to improve cybersecurity. Bill started his Federal career at NSA evolving from telecommunications to information assurance to cybersecurity.

Mr. Newhouse is a graduate of both the Georgia Institute of Technology and George Washington University and has been with the federal government for over 29 years.



Rodney Petersen

Director

National Initiative for Cybersecurity Education (NICE)

Rodney Petersen is the director of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST). He previously served as the Managing Director of the EDUCAUSE Washington Office and a Senior Government Relations Officer. He founded and directed the EDUCAUSE Cybersecurity Initiative and was the lead staff liaison for the Higher Education Information Security Council. Prior to joining EDUCAUSE, he worked at two different times for the University of Maryland - first as Campus Compliance Officer in the Office of the President and later as the Director of IT Policy and Planning in the Office of the Vice President and Chief Information Officer. He also completed one year of federal service as an Instructor in the Academy for Community Service for AmeriCorps' National Civilian Community Corps. He is the co-editor of a book entitled "Computer and Network Security in Higher Education". He received his law degree from Wake Forest University and bachelors degrees in political science and business administration from Alma College. He was awarded a certificate as an Advanced Graduate Specialist in Education Policy, Planning, and Administration from the University of Maryland.



Davina Pruitt-Mentle

Academic Lead

National Initiative for Cybersecurity Education (NICE)

Dr. Davina Pruitt-Mentle serves as Lead for Academic Engagement of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST). Prior to joining NICE, she was a senior researcher and policy analyst for Educational Technology Policy, Research and Outreach (ETPRO) and served as the Co-PI for the National Science Foundation (NSF) supported National Cyberwatch Center (NCC). Previous to NCC leadership, she served as faculty within the College of Education at the University of Maryland, College Park, and served as Director of Educational Technology Outreach within the College of Education at UMCP from 2001-2008. She has spent the past 20 years conducting research on student and educator cyberawareness, and developing programs to help increase the cybersecurity workforce pipeline. She received her Ph.D. in Educational Technology Policy from the University of Maryland, her M.Ed from Lynchburg College, and her B.S. from Virginia Tech.



Nasrin Rezai

Global Chief Information Security Officer

GE Capital &

GE Digital Security Governance, Tech Risk and M&A

Nasrin Rezai is GE Capital's Global Chief Information Security Officer and head of Corporate Governance, Technology Risk and M&A security, for the industrial GE businesses. In this role she is responsible for all aspects of cyber security management including incident response, threat intelligence, security management, operation, compliance.

Prior to joining GE, Nasrin was SVP Chief Technology Risk Officer in the Enterprise Risk Management Organization at State Street. In this role, she oversaw the creation of a technology risk management function to ensure effective, independent technology risk management governance, improved risk-based management decision processes and framework and automated processes and reporting.

Nasrin's other senior roles also included chief Technology Officer of Security for Cisco Sales and architecture function. In that role, she promoted thought leadership in security architecture and technology for Cisco's customers. She also led go to market strategies to embed security in cross architecture selling models. Other roles at Cisco also included responsibility for Cisco's global security vision, strategy, and architecture to protect the company's information and computing assets. In that capacity, she integrated leading-edge technologies and solutions — including borderless networking, "BYOD," virtualization and cloud computing — into the company's security architecture. With responsibility for the security architectures of Cisco's diverse businesses such as WebEx, Nasrin oversaw the development and management of the company's Software as a Service (SaaS) security model. Prior to Cisco, Nasrin held a series of executive-level positions at Hewlett Packard Corporation.

Throughout her career, Nasrin has promoted engineering, architecture in designing security solutions for large enterprises. She is passionate about helping others develop their potential, and mentors many young men and women. She holds a master's degree in business administration and a bachelor's degree in information systems. She holds an Executive Certification from Harvard and Cambridge.



Monica Ricci

Executive Producer, Content and Messaging
Katzcy Consulting, LLC

Throughout her career, Monica's method is to directly engage with customers and market experts to realize her mission: bringing insights and market awareness into an organization's strategy, roadmap and execution. She excels at bridging the expanse between technical teams and business leaders, positioning technology both to optimize business processes and to deliver intelligence, as well as translating business goals and objectives into technical requirements. Monica worked for over twenty years in the telecommunications industry, as a cellular radio engineer, an operations business analyst, a product manager and a director of marketing strategy. She has a BS in Physics from Santa Clara University and an MBA from the University of Chicago Booth School of Business.



Bernie Skoch
CyberPatriot National Commissioner

Brigadier General Bernie Skoch (USAF, Ret.) was named National Commissioner of CyberPatriot, the Air Force Association's National Youth Cyber Education Program, in 2010. Skoch graduated from the University of Arkansas in 1974 with a bachelor's degree in industrial engineering. Upon graduation he was commissioned as a second lieutenant in the Air Force. His 29-year Air Force career took him throughout the United States, Europe, Asia, the Pacific, and the Middle East on permanent and temporary duty until retiring at the rank of brigadier general.

Skoch has more than 20 years of experience in leadership positions developing, managing and implementing communications and information systems for the United States Air Force as well as the Defense Information Systems Agency (DISA). During his time at DISA he served as the Principal Director for Customer Advocacy and also as the Principal Director for Network Services. Within the USAF he served as Director of Mission Systems, Director of Communications Operations, and Director of Chief Information Officer Support where he was responsible for aligning information technology systems with business process improvements. He has developed policies for global telephone, video, radio, voice, data and satellite systems. Before joining CyberPatriot, Skoch was a consultant in the cyber and IT industry.

As Commissioner, Skoch oversees the planning and implementation of CyberPatriot and provides leadership and support for the program's development. In this role, Skoch is able to further student interest in science, technology, engineering and mathematics related studies, as well as increase their awareness of cybersecurity threats.

Bernie is an Instrument-Rated Commercial Pilot, an amateur astronomer, a marathon runner and a ham radio operator. Bernie and Debbie, his wife of 44 years, have six children and eighteen grandchildren, all residing in Northwest Arkansas.



Bobbie Stempfley
Director Cyber Strategy Implementation
The MITRE Corporation

Roberta “Bobbie” Stempfley is currently director of cybersecurity implementation at The MITRE Corporation. She is responsible for advancing MITRE’s cyber strategy, shaping the company’s cyber work program, executing the cyber business strategy, and raising awareness across the customer base. Most recently, Ms. Stempfley served in key leadership roles in the Department of Homeland Security, including deputy assistant secretary and acting assistant secretary for cybersecurity and communications. Previously, Ms. Stempfley was the chief information officer at DISA. Ms. Stempfley holds a B.S. in engineering mathematics from the University of Arizona and an M.S. in computer science from James Madison University.



Dr. Adam Tagert
Technical Director
NSA Science of Security Program

Adam Tagert is the Science of Security (SoS) Technical lead in National Security Agency Research Directorate. He works in all aspects of SoS particularly in the promotion of collaboration and use of foundational cybersecurity research. He promotes rigorous research methods by leading the Annual Best Scientific Cybersecurity Paper Competition and supports the SoS community as a frequent poster on the SoS Virtual Organization Site. Dr. Tagert received his Ph.D. from Carnegie Mellon University in Engineering and Public Policy where he researched national cybersecurity strategies of small developing nations, particularly Rwanda. He majored in Computer Science at Princeton University.



Greg Touhill

Deputy Assistant Secretary, Cybersecurity and Communications
DHS

Greg Touhill is one of the nation's premier cybersecurity and information technology senior executives. He is a highly experienced leader of large, complex, diverse, and global operations, and a senior US federal government official leading national programs to protect the United States and its critical infrastructure. A decorated combat leader, American diplomat, and senior executive with documented high levels of success on the battlefield and in the boardroom, Greg is an accomplished author and highly sought public speaker. In September 2016, he was named as the first ever federal chief information security officer, reporting to Tony Scott (federal CIO) and responsible for bolstering the government's digital defenses.





Dan Waddell

Regional Managing Director, North America Region
(ISC)², Inc.

Dan Waddell is responsible for managing (ISC)² operations in the North America Region, which primarily focuses on supporting our U.S. and Canadian members, customers and strategic partners with over 20 years of experience in information technology, information assurance, and cybersecurity. Dan has served in various management and leadership roles with (ISC)² for over 15 years. He has been a featured guest speaker on cybersecurity issues on both TV and radio shows such as “NBC News4 MIDDAY,” “Government Matters” and “Federal News Radio,” in addition to several cybersecurity conferences across the United States. He is currently a Fellow at the Institute of Critical Infrastructure Technology (ICIT), a non-partisan think-tank based in Washington, D.C. that acts as a conduit between the legislative community, technology providers and federal agencies. Mr. Waddell also chairs both the (ISC)² U.S. Government Advisory Council and the U.S. Government Executive Writers Bureau, and received the (ISC)² President’s Award in 2013.

During his consulting career, Dan’s clients included the Department of Transportation, Department of Defense, Department of State, Internal Revenue Service, Social Security Administration, Department of Health and Human Services and the Department of Homeland Security. Services provided included CISO/CSO advisory services, information security program management, secure cloud computing, security authorization, privacy, data loss prevention, information assurance, regulatory compliance, threat and vulnerability assessments, incident response, disaster recovery/business continuity, risk management and security engineering.



Dr. Gregory White

Director, Center for Infrastructure Assurance and Security (CIAS)
UT San Antonio

Dr. Gregory White has been involved in computer and network security since 1986. He spent 30 years with the Air Force and Air Force Reserves. He obtained his Ph.D. in Computer Science from Texas A&M University in 1995 conducting research in the area of computer network intrusion detection and he continues to conduct research in this area today. He currently serves as the Director of the Center for Infrastructure Assurance and Security (CIAS) and is an Associate Professor of Computer Science at The University of Texas at San Antonio (UTSA).

Dr. White has been involved in security instruction for many years. He taught at the U.S. Air Force Academy for seven years where he developed and taught courses on Computer Security and Information Warfare. He helped build the nation's first undergraduate information warfare laboratory while at the Academy and twice received the Academy's Computer Science Research Excellence Award. At UTSA Dr. White continues to develop and teach courses on computer and network security. He has also been very active in the development and presentation of cyber security exercises for states and communities around the nation and with the development of training designed to help states and communities develop viable and sustainable cyber security programs. He very active in development of cyber security competitions and was instrumental in the development of NCCDC and CyberPatriot.

Dr. White has written numerous articles and conference papers on computer security. He is also the co-author for five textbooks on security and has written chapters for two others. His current research interests include an examination of organizational issues affecting computer security, high-speed intrusion detection, infrastructure protection, community cyber incident response, and the development of the Community Cyber Security Maturity Model (CCSMM).

