Cyber-Securing Super Bowl 50: What Can a Live-Fire Football Match Teach Students about Becoming Better Cybersecurity Professionals?

MW Bovee, HOL Read

Computer Science/Computer Security & Information Assurance
School of Business & Management
Norwich University
Northfield, Vermont, United States

Email: mbovee@norwich.edu; hread@norwich.edu

Abstract: *The rise and regularity of cybersecurity incidents have increased the demand for trained workforce professionals. Institutions of higher education have responded by including practical hands-on exercises such as capstones, labs, and simulated attack-and-defend 'Capture-the-Flag' scenarios. Many degree programs also encourage students to gain experience via internships. This paper considers real-world experience gained by students through another means—by assisting law enforcement personnel in defending Super Bowl 50 cyberspace. This annual game, with high security requirements and international prominence, provided a unique opportunity to reflect whether 'live-fire' experiences can improve technical and professional skill sets of students who are emerging from higher-education into the workforce.*

Keywords: *Cybersecurity, Experiential Learning, Professionalism, Curriculum*

Introduction

In the United States, the Super Bowl is an annual, internationally-prominent, sports-related, mass gathering. It is the culminating event of the American professional football season, and routinely draws stadium crowds in excess of 80,000 plus an international audience of over 100 million watching the event on television (Grossi 2014). In 2002, in the wake of the September 11th atrocities, the visibility and significance of the event resulted in its being designated by the United States President as a National Security Special Event (NSSE) (United States Government 18 U.S.C. § 3056[e]). Because of its magnitude and significance, the Super Bowl is routinely classified as a Special Event Assessment Rating of 1 (SEAR 1)—an event that warrants the support of the American Government (Reed n.d). As a SEAR 1 event, the 50th annual Super Bowl (Super Bowl 50, or 'SB50') involved a number of organisations, including: the Federal Bureau of Investigation, the Department of Homeland Security, the Secret Service, Customs and Border Control, the U.S. Postal Service, the Transportation Security Administration, the Federal Aviation Administration, the U.S. Air Force, and the U.S. Coast Guard—all led by the Santa Clara Police Department (SCPD) (Grossi 2014).

Super Bowl 50 was hosted by Levi's stadium in Santa Clara, California. This stadium was designed and constructed with 1200 WiFi hotspots and bandwidth (40 gigabits per second) to allow all guests simultaneous, real-time WiFi access during games. There are sufficient connections—40 times that of any other stadium in the U.S.—for it to be considered one of the most high-tech sports venues to date (Bajarin 2014). Such infrastructure also supports emergency services, crowd control, and the evolving 'fan experience' of such activities as watching instant replays and ordering products that are then delivered to the fans at their seat while in the stadium (Martin 2016).

Within this environment, a cohort of 65 students drawn from predominantly Computer Science (CS) and Computer Security and Information Assurance (CSIA) majors worked to assist the SCPD in developing and implementing solutions to protect and defend the 'cyberspace' of the SB50 event from any would-be assailants looking to damage the reputation of those involved, to cause disruption in the fan experience, or to prevent any other attackers with sinister motives. The focus of this paper is on the experience gained from the perspective of the students. The paper considers whether real-world exercises such as this are of merit, whether they improve student knowledge of working in the cyber field, and whether they help to prepare students for future work in the cyber workforce.

In the next section, entitled 'Related Work', the authors examine the developing need of cybersecurity education and the move towards incorporating more practical experience. The section entitled 'Contribution' highlights the contribution of this paper to the field of cybersecurity education; 'Methodology' details the project structure and processes for engagement with Super Bowl 50; and 'SB50 Project Development' describes the process taken to identify new learning by student participants. The section called 'Discussion' considers the results of new learning by students, and 'Conclusions' provides closing remarks about the overall project.

Related Work

The idea of universities and similar institutions teaching cyber-related curricula is not new. The first undergraduate degree to feature the term 'hacking' appeared in 2006 (Abertay 2016), while many programs in information security were available as far back as the 1990s (Kessler & Ramsay 2013). The typical forms of teaching cyber within higher-education institutions have since aggressively moved away from the more traditional forms of teaching (lectures, reading literature, understanding concepts in principle) as students often cannot apply the academic principles they have learned to a realistic environment (Willems & Meinel 2012). Available literature in the public domain shows that the 'Capture-the-Flag' (CtF) genre, whereby a specific aim or goal is set, typically for an offensive exercise such as obtaining a particular file from a system, has remained very popular as an educational tool to help students understand how to configure, respond, defend, attack, and exploit networked systems. Indeed, many security organisations have taken to using this model of 'gamification' (Herr & Allen 2015) as a recruiting tool, including government, as seen in the Government Communication Headquarters (GCHQ 2011) and the National Security Agency (NSA 2014). Others encourage a team-based model of this approach. Conklin (2007) describes an information security practicum course whereby students, working as part of a team, make amendments in a simulated small business environment. Changes are issued via memos and outside of student class time (for example, by introducing malware or the 'accidental' deletion of a file). The real-world simulation is kept by maintaining system states between classes (thus, providing the sense of continuity), by incorporating the input of industry professionals (thus, preventing the instructor from doing the 'same old thing'), and by focusing on the business (thus, preventing students from treating them like their 'personal playgrounds') (Conklin 2007). Rege (2015) applies cyber curricula to students without a strong background in computing (criminal justice majors). Such students encounter issues with the prevailing CtF model, namely novice encouragement, temporal constraints, and skewed experiences (barriers to entry based on prior knowledge).

Similar practical educational exercises have been developed for other, more focused areas within the cyber realm. Sitnikova, Foo, and Vaughn (2013) discuss their experiences taking the experiential model in cybersecurity learning and applying it to the realm of Supervisory Control and Data Acquisition (SCADA) systems. Practical exercises were designed which helped to maximise student education of cyber within this area while minimising the amount of time needed overseas at specialist training facilities.

Dopplick (2015) nicely sums up these worldwide trends in experiential cybersecurity learning: technical project-based activities, competitions, training and research are becoming commonplace as are universities "teaming with companies to provide structured programs on an ongoing basis" (84). Such exercises focus on providing simulated, controlled, safe, and legal, opportunities for student practice (National Institute of Standards and Technology [NIST] 2018a; NIST 2018b). Yet the recommendations of the USA National Initiative for Cybersecurity Education (NICE) exhort the need to challenge the assumptions and analyse the rationale for past, present, and proposed future cybersecurity education; and, inspire, explore, and experiment, with creative, innovative approaches to education, even to the degree that they might "disrupt or defy the status quo" (NIST 2016, n.p.).

The SB50 engagement serves as one such possible innovative or disruptive approach to cybersecurity education. A review of available literature indicates SB50 is one of the few times that students have been directly involved in providing cyber-capability for such a high-profile, high-risk event. At best, students have traditionally been involved in more of an 'observational' role with limited direct input. Many students have gained practical experiences while working in internships over a period of ten weeks or so (NIST 2018c). However, internships cannot guarantee intensive periods during which there is a heightened sense of imminent cyberattack. The intense focus of analysing data and responding in real time to possible threats is simulated in competitions (for example, CtF). However, knowing that it is indeed a simulation often leads to a cavalier approach that would not be acceptable under duress in a real-world attack-and-defend situation (for example, aggressively changing firewall rules that block the threat actor, but inadvertently also preventing real users from carrying out essential business activities). The NICE Cybersecurity Workforce framework itemises recommended or required cybersecurity skills and abilities related to communication, collaboration, and teamwork (**Table 1,** below). Many of these directly relate to the experiences noted and comments made by students who participated in the Super Bowl 50 project. However, nowhere does the NICE framework specifically address the need to work effectively under urgent decision-making conditions. Student participation in cybersecurity at an event such as Super Bowl 50 had the advantage of the students' experience of the heightened awareness that accompanies the threat of attack on an organisation, rather than a simulated threat.

Number	Description
S0070	Skill in talking to others to convey information effectively (note this does not really imply collaboration or communication, merely conveying information clearly)
S011	Skill at interfacing with customers
S0244	Skill in managing client relationships
S0301	Skill in writing about facts and ideas in a clear, convincing, and organized manner
S0341	Skill to articulate intelligence capabilities available to support execution of the plan
S0315	Skill to articulate the needs of joint planners to all-source analysts
S0343	Skill to orchestrate intelligence planning teams, coordinate collection and production support, and monitor status
S0356	Skill in communicating with all levels of management including Board members (such as interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
A0011	Ability to answer questions in a clear and concise manner
A0013	Ability to communicate complex information, concepts, or ideas, in a confident and well- organized manner through verbal, written, and/or visual means.
A0074	Ability to collaborate effectively with others
A0076	Ability to coordinate and collaborate with analysts regarding surveillance requirements and essential information development
A0077	Ability to coordinate cyber operations with other organizational functions or support activities
A0078	Ability to coordinate, collaborate, and disseminate, information to subordinate, lateral, and higher-level, organizations.
A0082	Ability to effectively collaborate via virtual teams
A0098	Ability to participate as a member of planning teams, co-ordination groups, and task forces, as necessary.

Table 1. Skills and abilities from the NICE Cybersecurity Workforce Framework that are related to 'live-fire' educational opportunities (Newhouse et al. 2017)

SB50 Project Development

Initial contact and invitation

To identify smaller real-world engagement opportunities for capable students, faculty of the School of Business & Management CS and CISA programs had, for years, been leveraging contacts through alumni and through state, federal, and professional organisations. Early in the spring of 2015, a high-level alumnus reached out to a leading faculty member of the program as a Point Of Contact (POC) and invited cybersecurity student participation as SB50 observers. During the remainder of the spring semester, a selected team of students led by the POC researched similar previous high-level events, evaluated what program students could potentially offer as value-added event support, and made site visit plans.

Initial site visits and proposed expanded role

As both an information-gathering and experiential-learning exercise, in early summer the faculty POC and student team travelled to the SB50 event site and observed site-security operations for several significant sporting and entertainment events. Using information gathered, prior research, and forecasts of possible added value, the team proposed providing several services to support event cybersecurity. Based on the quality of their preparation and the proposed services, the role of the student team to be fielded for the event was elevated from merely observing to actively contributing to the effort. Subsequently, additional site visits were conducted to test proposed services and associated proof-of-concept equipment.

Creating the team

This project presented unique real-world experiential learning opportunities for students, including a window into security issues for a SEAR-1 event; interaction with high-level security professionals; and provision of professional-quality cybersecurity support for an internationally-prominent event. The goals of the project were, therefore, to maximise the number of students who could appropriately participate, to maximise their opportunities to do so, and to stress professionalism and value-added quality for the event.

Due to the high-profile nature of the engagement (an ‘academic exercise’ for a significant, real-world, live-fire event), a senior faculty member acted as Project Manager (PM). The PM was responsible for project administration and troubleshooting; for guiding the project team; and for serving as project liaison with event leadership, University administration, and supporting vendors.

The nature and scope of the goals and services necessitated a team structure comprised of six subteams by area (Area Teams) with the following responsibilities:

- Operations—this group worked with the PM on areas such as team coordination and communication, and to clarify and communicate information of significance to SB50 decision-makers on the day of the event;
- Technical—these students were responsible for project system analysis and design, specialised hardware and software implementation, and database administration and management;
- Infrastructure—this group was responsible for the operation and maintenance of University research centre hardware and software that supported specialist project systems;
- Information Gathering—these students were in charge of surveillance, aggregation, and distillation of open-source information regarding the event and for identifying potential security issues;
- Site Security—this group focused on the University site and personnel security for operations during the engagement; and,
- Communications—these students served as public relations liaisons between Project/Area Teams, the University, SB50 leadership, and public media.

Students who had participated in the summer site visits, who had prior experience or skills, or who had demonstrated the capability for mature leadership were selected to lead the Area Teams (Team Leads). Several had already been contributing to the project since the initial spring alumnus contact; several stepped up at the start of the fall semester. Faculty with specific expertise acted as subject matter experts and POCs for the Area Teams.

Due to the sensitive nature of the engagement and the data that would be observed, the Communications Team was tasked with writing a first draft Non-Disclosure Agreement (NDA) with Levi's Stadium. The first draft was then refined by the PM in collaboration with them, with SCPD, University administration, and legal counsel. Because of the notoriety of SB50, it was also anticipated that many students would offer to participate on the Project Team regardless of their ability to do so. For example, students might have had the skills and maturity but not the free time unless they jeopardised their academic progress or other responsibilities. Others might have had the free time but lacked the maturity to maintain operational security or professionalism. The PM, therefore, wrote a Memorandum Of Understanding (MOU) to ensure students grasped and acknowledged the importance of balancing project participation with their other responsibilities, as well as the professional behaviour expected of all project team members.

Due to the unique learning opportunity presented by SB50, it was decided early on to include as many students in the experience as feasible. An open invitation was broadcast to all students and a large lecture hall was used to introduce the project. The PM and Team Leads presented the project opportunity and scope, the Area Teams, and the professionalism expected of participants. Interested students signed up, listed their preferred Area Teams, and noted any special skills or abilities they had that were relevant to the project. Team Leads identified those students best suited to supporting the various project areas, consulted with the PM, and issued invitations to the respective students. Sixty-five students, primarily CS and CSIA majors, formed the overall project team. Some students with a broad range of skill, ability, and interests participated in more than one support area. All project team members were given counselling on appropriate channels of communication regarding project inquiries and on maintaining operational security. They were also required to sign an NDA and MOU (which were then countersigned by the PM on behalf of the University).

Security operations and the many federal, state, local, and industry support groups at SEAR-1 events require considerable space, resulting in limited 'seating'. The Project Team was, therefore, structured for the eventuality of needing a small group on-site (dubbed the 'Away Team'). This consisted of an experienced CSIA faculty mentor, a staff member from university PR, and the minimum number of Team Leads needed to support on-site event cybersecurity. The rest of the Project Team that remained behind was dubbed the 'Home Team'. The Away Team was expected to provide direct cybersecurity support at the event site; act as liaisons, interpreting and coordinating requests to/from event leadership; and, coordinate and interpret information flow from the Home Team. The Home Team was responsible for providing behind-the-scenes support for the Away Team, for maintenance and operation of project infrastructure, for continuous monitoring of observed information, for addressing event leadership requests for information, and, for summarising and communicating back any information on potential threats or in response to direct requests.

Away Team members were Team Leads from Operations, Technical, and Communications. Consequently, these individuals took on the added responsibility of identifying and training 'seconds': individuals capable of leading the respective Home Team Area activities once the teams separated.

Pre-Event preparation

In the fall semester, several pieces of specialised equipment were installed on site and were tested both locally and remotely. During this same period, Project Team students conducted preparatory activities ranging from software, database, and infrastructure development, to learning about nuances managing PR for a major event. Dry-run exercises were conducted to develop and debug procedures, and to train and prepare students, teams, and team leaders.

For this event, the extensive preparation and run-up was interrupted for almost a month due to the winter break. The PM and several Team Leads remained active during the break. However, once

the spring semester began, it was necessary to reconvene the Project Team and re-establish team cohesiveness rapidly.

As part of event preparation, an early on-site Table-Top Exercise (TTX) was held to simulate various levels of incident criticality, and to surface security issues for consideration and resolution. The PM represented the university at the initial TTX and, with approval, communicated the simulation scenarios and key issues to the Project Team. To help students with responsibility for team leadership better understand the complexity of such multi-agency event support, they and the PM observed an actual cybersecurity TTX at the Vermont Emergency Operations Center. Finally, in preparation for SB50, those same students conducted a TTX to brainstorm and troubleshoot anticipated problems with supporting security for the live event, such as issues with hardware, software, or communication glitches; planned processes or procedures; communication and coordination within Area Teams; and coordination between the Home and Away Teams.

One week to go

The real-world exercise involved collaboration and communication at many levels, in different contexts, and with a variety of law enforcement and technical professionals as well as within student teams. This was especially true in the final week run up to, and the weekend surrounding the event.

To coordinate with event leadership and agency support, the Away Team travelled to the site a week before the event. The team coordinated with event leadership and representatives of various law enforcement groups, professional technical experts, and public relations personnel. Operations and Technical members of the team also collaborated with Levi's Stadium IT to assure technical and procedural readiness, while Communications members of the team supported event PR. During this time, the Home Team tested project systems, team readiness, and real-time communications with the Away Team by conducting daily dry-run sessions 6 PM to 10 PM Monday through Thursday.

During the event

The Home Team stood up full operations at 6 PM on the Friday before game day. Predetermined rosters of Home Team students working in each Area Team, supervised by the PM and several faculty POCs for Area Teams, supported shifts around the clock. During this time, the Away Team shifted roles. The Communications members acted as an on-site extension of the Information-Gathering team, while the Technical and Operations members monitored and evaluated data from site instruments and coordinated with the Home Team for requests from event leadership. In general, the Away Team was embedded with federal, state, and local law enforcement, public safety, and stadium technical personnel and stood ready to respond to specific tasks. During the event, several questions, issues, and items of interest arose; and requests from SB50 law enforcement to act on them were relayed from the Away Team Operations Leader to the appropriate Away Team or Home Team subgroup, and in some cases to both. Leaders for the Home Team received the relayed tasks and had to coordinate their specific team activities to generate results that were accurate, substantive, and timely. Furthermore, they had to work within the overall Team structure to provide clear, concise, appropriate responses in support of a high-risk, high-profile event. In short, they were under considerable pressure to collaborate and communicate, and to 'get it right' in many senses of that phrase. Event cybersecurity support was maintained for approximately 60 hours, until a post-game 'all clear' order from SB50 event leaders was received the following Monday morning.

Post-Event

Participation in the event generated local media interest. As a result, once operational security was no longer a concern, several Team Leads participated in local PR opportunities. The Technical and Infrastructure teams collated data collected from the event and created backup copies of the aggregated data. Finally, all Project Team students were invited to participate in a post-event questionnaire.

Evaluation Methodology

Engaging in cybersecurity at such a significant event certainly comes with its own rewards for students. Beyond kudos, however, it is important to consider how such an exercise lends itself to improving student Knowledge, Skills, and Abilities (KSAs), and their professionalism. To gauge the event's effectiveness as a learning tool, participants were invited to complete a survey with open-ended questions rather than having them select from a specific set of keywords or Likert scale choices.

The questions focused on three key areas. First, to identify what and where their skills came from, students were asked to evaluate their prior knowledge and level of preparedness for the event (Questions 1-3 in **Table 2**). Second, to identify their expectations for engaging in the project, students were asked what they had hoped to gain by participating (Question 4, **Table 2**). Third, to gauge benefits of participating, students were asked to reflect upon the experience and of their learning (Questions 5-6 in **Table 2**). To allow the cohort a reasonable period of reflection about what they personally achieved from the exercise, the survey was distributed at the end of the spring 2015 semester to all student participants in the SB50 event.

Survey Questions						
Descriptive Terms	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**
Academic Classes	73.3					
Clubs & Societies	13.3					
CtF Competitions	6.7					
None	6.7	8.3	15.4			
Internships		16.7				
Communication		25				19.2
Organization		8.3				
Leadership		16.7	7.7	7.7		26.9
Technical		25	38.5	15.4		26.9
Practical Exp.			23.1	76.9		11.5
Confidence			15.4			
Teamwork					100	15.4

Table 2. Categories of terms used by students to describe their preparedness, expectations, and reflections regarding Super Bowl 50 event participation; all results are a percentage of each question (column) total
Legend: Q1 – Prior knowledge of cybersecurity; Q2 – Prior preparations; Q3 – Areas that were lacking; Q4 – Expected KSAs required; Q5 – Memorable moments; and, Q6 – KSAs gained post-event

Of the 65 students who took part in the Super Bowl 50 project, 25% responded to the questionnaire. The low response rate may have been due, in part, to a variety of circumstances: over half the project team consisted of first- and second-year students, there was no 'before' survey circulated prior to the event to set expectations of a follow-up, a response bias may have favoured those students who took on added responsibility as leaders of the various project team sub-groups, or the end-of-spring distribution point came at a time when students were either distracted by ongoing academic activities or so far post-event as to be less motivated to give feedback.

Responses for each question were examined for the descriptive terms used and the terms categorised. The gist of each question and the extrapolated answers are presented in Table 2, above. (Values shown are percentages of categories provided as answers.)

Discussion

Prior knowledge/preparedness (Questions 1-3)

Question 1 sought to elicit student perceptions about the cybersecurity profession, particularly the skills the students deemed most important. Question 2 and 3 together also sought similar information but were framed by the context of this particular project (Super Bowl 50).

When asked what they knew about cybersecurity as a profession before involvement with the exercise, most respondents used terms indicating technical skills obtained from lab-based academic learning (73.3%), from extra-curricular activities (such as campus clubs and professional societies; 13.3%), from CtF experiences (6.7%). A small percentage (6.7%) indicated that they had no prior knowledge. Of interest was the near-unanimous focus on technical ability. There were no indications of any ‘soft’ skills, such as interpersonal collaboration or communication, as highlighted by the NICE Cybersecurity Workforce framework (**Table 1,** above).

When asked what KSAs prepared participants for the SB50 project, students still emphasised technical skill (25%), but also anticipated a need for those ‘soft’ skills, such as: communication (25%), leadership (16.7%), prior professional experience (internships; 16.7%), and organisational skills (8.3%). A few (8.3%) felt they had no KSAs that prepared them for the experience. Overall, technical ability now only accounted for a quarter of the responses (**Table 2,** above).

When considering areas in which they felt they were lacking, most of the respondents again focused on technical ability (38.5%) and prior professional experience (23.1%). Confidence (15.4%) and leadership (7.7%) were the only other soft-skill areas highlighted (**Table 2,** above).

Expectations of the event (Question 4)

Question 4 prompted students to describe the skills they believed were needed to undertake the SB50 project. Technical skills only accounted for 15.4% of the responses, with practical experience taking the largest percentage at 76.9%. References to practical experience included terms such as “real world experience”, “how cyber plays into big events”, “understanding security requirements”, “working on a large scale project”, and “how events are run and secured”. Technical ability was still a core part of the answers, but the terms used also fit communication, organisation, and management abilities (**Table 2,** above).

Reflection on experience and learning (Questions 5 and 6)

Question 5 allowed the students to describe, in their own words, what was most memorable about being part of SB50. Question 6 sought the same information, prompting students to consider any KSAs obtained.

Students unanimously answered that the teamwork required was the most memorable aspect of working on SB50. Although some technical abilities were mentioned in passing, no respondent explicitly highlighted any new technical skills or abilities he or she acquired during the project. Asking the students to focus on KSAs they obtained helped explicate what “teamwork” meant to them in this context: technical and leadership skills (26.9% each), communication (19.2%), peer collaboration (15.4%), and practical experience (11.5%) (**Table 2**, above).

Results Interpretation

The purpose of this questionnaire was to assess if there was academic merit to students engaging in planning, organising, and participating in an event such as Super Bowl 50. Events such as these could be an innovative or disruptive approach to cybersecurity education by providing the focus and intensity of a CtF with the professional experience obtained during an internship.

Before participating in Super Bowl 50, students tended to consider cybersecurity an almost exclusively technical discipline. However, upon being asked what skills were needed for such a project, soft skills were identified (communication, leadership, organisation). The teamwork needed for an event of this magnitude and scope was, unanimously for students, their most salient memory. However, when asked to consider new KSAs obtained, only one quarter highlighted new technical abilities. The remainder highlighted skills expected of young professionals entering the workforce. The nature of the exercise, the team structure to cope with it, and the interaction necessary within the team and with external professionals from a variety of disciplines appear to have stressed the critical nature of collaboration and communication—the so-called ‘soft skills’ in cybersecurity.

Conclusions

This paper presented a unique opportunity undertaken by a student cohort—having assisted in defending cyberspace during Super Bowl 50. Students began working a year in advance on a wide range of event preparations that culminated in a focused, intensive week capped off by around-the-clock support before, during, and after the game. A review of existing literature did not reveal similar engagements in which students provided active support alongside law enforcement and other personnel; at most students have been given observational opportunities. Thus, this engagement serves as a potential example of an innovative new approach to cybersecurity education. Given the limited data, do such real-world event processes and opportunities merit recommendation to other academic institutions? Would students seeking employment in the cybersecurity sector gain knowledge, skills, or abilities that improved their ability to perform in industry, or would the exercise be simply a novel distraction?

The prior build-up to the event allowed students to experience the extensive range of advance thought, preparation, organisation, and management that can go into defining, creating, and implementing real-world cybersecurity for a professional engagement. There was a clear focus and intensity felt by participants very much akin to Capture-the-Flag competitions. Several students described it this way: “During this project I have never been so tired, so frustrated, so mad, so proud, or so happy”; “I gained technical skills, administration skills, leadership skills, communication skills, all of it”; “I got the shared sense of accomplishment and bonding”; and “I learned how to be flexible and multitasking and how to work when I was tired”.

However, unlike CtF, intense cybersecurity coverage began well before the real-world event and continued until well after the event ended. Also, cavalier attitudes towards the engagement were discouraged by faculty mentors and recognised by students as a real-world risk. This tempered student actions. Through it all, students gained potentially valuable experience at something not mentioned in the NICE Cybersecurity Workforce Framework—a context of urgent, critical decision-making. The heightened sense of criticality related to the actions they performed and information they conveyed, as well as the impact on real-time decision-making and the time-pressure of the ‘live-fire’ event, provided the students the sort of novel, innovative, and possibly disruptive educational opportunity invited by the NICE Strategic Plan (NIST 2016). The process was also particularly scalable; the cohort included all computer science and cybersecurity students with the time and interest to participate, and even a handful of non-computing majors who wanted to learn more about cybersecurity through practical experience. Voluntary, anonymous feedback from student participants suggested they gained experiences like those that might be expected from professional internships. Finally, their responses also suggested an apparent shift in perceptions from a tech-centric view of cybersecurity to one involving important, so-called ‘softer’ professional project skills. Engagement in a real-world situation emphasised the need for effective collaboration and communication. To the degree that exercises, scenarios, or simulations can emulate for students the same real-world teamwork pressures, they may impart similar student insights and help better prepare cybersecurity professionals for their future roles.

References

Abertay University 2016, ‘Ethical hacking’, viewed 23 December 2018, <https://web.archive.org/web/20160324125042/http://www.abertay.ac.uk/studying/ug/ ethhac/>.

Bajarin, T 2014, ‘Meet Levi’s Stadium, the most high-tech sports venue yet’, *Time,* viewed 23 December 2018, < http://time.com/3136272/levis-stadium-tech/>.

Conklin, A 2007, ‘The design of an information security practicum course’, *Proceedings of the AIS SIG-ED IAIM Conference*, Montreal, CA.

Dopplick, R 2015, ‘Experiential cybersecurity learning’, *ACM Inroads*, vol. 6, no. 2, p. 84.

Government Communications Headquarters (GCHQ) 2011, ‘Behind the code’, viewed 23 December 2018, <http://www.canyoucrackit.co.uk/>.

Grossi, D 2014, *Mass gathering security: A look at the coordinated approach to Super Bowl XLVIII in New Jersey and other large-scale events*, U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications, viewed 23 December 2018 <https://democrats-homeland.house.gov/sites/democrats.homeland.house.gov/files/sitedocuments/20140623094446-10021.pdf>.

Herr, C & Allen, D 2015, *Video games as a training tool to prepare the next generation of cyber warriors*, Carnegie Mellon University, Pittsburgh, PA, US, viewed 23 December 2018, <https://resources.sei.cmu.edu/asset_files/Presentation/ 2015_017_001_442344.pdf>.

Kessler, GC & Ramsay, J 2013, ‘Paradigms for cybersecurity education in a homeland security program’, *Journal of Homeland Security Education*, vol. 2, pp. 35-44, viewed 23 December 2018, <http://www.journalhse.org/v2-kesslerramsay.html>.

Martin, R 2016, *Super Bowl 50 tightens cybersecurity,* Vermont Public Radio, viewed 23 December 2018, <http://www.npr.org/2016/02/07/465901857/super-bowl-50-tightens-cybersecurity>.

Newhouse, W, Keith, S, Scribner, B & Witte, G 2017, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, National Institute of Standards and Technology (NIST) Special Publication 800-181*, Gaithersburg, MD, US, viewed 3 January 2019, <https://doi.org/10.6028/NIST.SP.800-181>.

National Institute of Standards and Technology (NIST) 2016, *National Initiative For Cybersecurity Education strategic plan*, Gaithersburg, MD, US, viewed 23 December 2018 <https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan>.

——2018a, *NICE Cybersecurity competitions*, viewed 23 December 2018, <https://www.nist.gov/sites/default/files/documents/2018/09/24/cybersecurity_ competitions.pdf>.

——2018b, *NICE Cyber ranges*, viewed 23 December 2018, <https://www.nist.gov/sites/default/files/documents/2017/05/23/cyber_ranges_2017.pdf>.

——2018c, *NICE Cybersecurity apprenticeships*, viewed 23 December 2018, <https://www.nist.gov/sites/default/files/documents/2018/01/09/ nice_apprenticeship_one_pager_oct_31_2017.pdf>.

National Security Agency (NSA) Careers 2014, *tpfccdlfdtte pcaccplircdt dklpcfrp?qeiq lhpqlipqeodf gpwafopwprti izxndkiqpkii krirrifcapnc dxkdciqcafmd vkfpcadf*, #MissionMonday #NSA #news, Twitter, 5 May 2014, viewed 23 December 2018, <https://twitter.com/NSACareers/status/463321993878994945>.

Reed, K n.d., *User's manual for National Special Security Events (NSSE)/Special Event Assessment Rating events (SEAR) Job Aid*, viewed 23 December 2018, <https://homeport.uscg.mil/Lists/Content/Attachments/2718/Users%20Manual%20for%20NSSE%20Job%20Aid.pdf>.

Rege, A 2015, 'Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation', 2015 *Summit on Gaming, Games, and Gamification in Security Education – 3GSE, USENIX*, August 11, Washington, D.C., US, viewed 3 January 2019 <https://www.usenix.org/system/files/conference/3gse15/3gse15-rege-update.pdf>.

Sitnikova, E, Foo, E & Vaughn, RB 2013, 'The power of hands-on exercises in SCADA cybersecurity education', *Proceedings of the Information Assurance and Security Education and Training. WISE 2009, IFIP Advances in Information and Communication Technology*, vol 406, 8-10 July, Auckland, NZ, Springer, Berlin, DE, pp. 93-94.

United States Government n.d., *Crimes and criminal procedure: Powers, authorities, and duties of United States Secret Service*, 18 U.S.C. § 3056(e).

Willems, C & Meinel, C 2012, 'Online assessment for hands-on cybersecurity training in a virtual lab', *Proceedings of the 3rd IEEE Global Engineering Education Conference (EDUCON 2012)*, IEEE Press, Marrakesh, MA.

Authors

Burhan Al-Bayati is currently a final-year PhD candidate at the Centre for Security, Communications & Network Research at the University of Plymouth (UK). He holds a BSC in computing from Baghdad University (Iraq), 2002, and an MSC in computing from Pune University (India), 2008-2010. Burhan's research interests include information security, biometric authentication, and cloud security.

Jonathan Z. Bakdash received the PhD degree in psychology in 2010 from the University of Virginia. He is a Research Psychologist with the Human Research and Engineering Directorate, U.S. Army Research Laboratory, South Field Element, at the University of Texas, Dallas. His research interests include human decision-making, human-machine interaction, and cyber security.

Dr. Andrew Blyth, formally the Director of the Information Security Research Group at the University of South Wales, has functioned as an expert witness in computer forensic and data recovery for a wide variety of law enforcement agencies, such as the Home Office, SOCA, and the Metropolitan Police. Dr. Blyth has also published several journal papers in the areas of computer forensic and data recovery, and is one of the leading global authorities on data sanitization and forensic techniques on solid state media. Dr. Blyth is on the ISO advisory board for standards relating to Computer Forensics, is a member of the National IA forum, and works with UK government agencies, including the Defence Science Technology Laboratory.

Dr. Matthew Bovee is the Associate Director of the Computer Science/Computer Security & Information Assurance program at the Norwich University School of Business & Management. As Lecturer there, he teaches general and specialist courses in computer science, digital forensics, and computer security. In addition to cyber security and digital forensics, Dr. Bovee's background includes research, publications, and degrees in accounting and information systems and exercise physiology.

Filipe Caldeira is an Adjunct Professor at the Informatics Department of the Polytechnic Institute of Viseu, Portugal. He obtained his PhD degree in Informatics Engineering in 2014 from the Faculty of Sciences and Technology of the University of Coimbra. He has acted as program director of the Informatics Engineering program since 2014. He is also a researcher at the Centre for Informatics and Systems of the University of Coimbra and at the CI&DETS research center of the Polytechnic Institute of Viseu. He has been recently involved in some international and national research projects.

Professor Nathan Clarke is a Professor in Cyber Security and Digital Forensics at the University of Plymouth. He is also an adjunct Professor at Edith Cowan University in Australia. His research interests reside in the areas of information security, biometrics, forensics, and cloud security. Professor Clarke has over 200 outputs consisting of journal papers, conference papers, books, edited books, book chapters, and patents. He is the Chair of the IFIPTC11.12 Working Group on the Human Aspects of Information Security & Assurance. Professor Clarke is a chartered engineer, a fellow of the British Computing Society (BCS), and a senior member of the IEEE.

João Henriques is a PhD student in Science and Information Technology at the University of Coimbra (UC) and Assistant Professor at the Department of Informatics Engineering at the Polytechnic Institute of Viseu (IPV). His research interests at the Center for Informatics and Systems at UC (CISUC) include forensic and audit compliance for critical infrastructures protection. He also remains a Software Engineer in the private sector.

Dr. Victor Jaquire has been within the field of cyber and information security for over 20 years within government and the private sector focusing on strategy, performance management, and operations. He holds an Honors Degree in Management from Henley University and a master's and PhD in Informatics from the University of Johannesburg--specializing in strategies for cyber counter-intelligence maturity and the security of cyberspace. He has published various academic papers on cyber strategies and cyber counter-intelligence maturity. His professional certifications include CISSP, CISM, and CCISO.

Fudong Li is a lecturer in Cyber Security at the University of Portsmouth, in the UK. Dr. Li is also a visiting lecturer at the University of Plymouth. His research interests are in the areas of biometric authentication and digital forensics; he has over 50 conference papers and journal articles in those domains.

Dr. John McAlaney is a Chartered Psychologist, Chartered Scientist, and Principal in Psychology at Bournemouth University in the UK. His research focuses on the social psychological factors of risk behaviors, including cyber security from the perspective of the attackers, the targets, cyber security practitioners, and other stakeholders.

Glenn Nor has a background in IT network and security, and completed one of Norway's first bachelor degrees that focuses specifically on digital forensics. He is now head of forensic technology services at PwC Norway and pursuing an MPhil/ PhD at the University of South Wales.

Dr. Huw Read is an associate professor at Norwich University and the director for the Centre of Advanced Computing and Digital Forensics (NUCAC-DF). Dr. Read began his academic career in 2004 at the University of South Wales (UK) and has taught several specialist courses in digital forensics and cyber security. For over ten years, he has worked alongside industry as well as government on a number of cyber-related projects, partnering with diverse teams to design solutions to complex security problems. Dr. Read is actively engaged in research and scholarship within the field, having published a number of research articles in journals and spoken at various cyber-related conferences.

Dr. Char Sample is a research fellow employed for ICF International at the US Army Research Laboratory in Adelphi, Maryland, and is also with the University of Warwick, Coventry, UK. Dr. Sample has over 20 years' experience in the information security industry. Most recently, Dr. Sample has been advancing the research into the role of national culture in cybersecurity events. Presently, Dr. Sample is continuing research on modeling cyber-behaviors by culture; other areas of research are information weaponization, data fidelity, and deception.