HAL
archives-ouvertes.fr

Developing Cyber Competition Infrastructure Using the SCRUM Framework

Heath Novak, Daniel Likarish, Erik Moore

▶ **To cite this version:**

Heath Novak, Daniel Likarish, Erik Moore. Developing Cyber Competition Infrastructure Using the SCRUM Framework. Ronald C. Dodge; Lynn Futcher. 8th World Conference on Information Security Education (WISE), Jul 2013, Auckland, New Zealand. Springer, IFIP Advances in Information and Communication Technology, AICT-406, pp.20-31, 2013, Information Assurance and Security Education and Training. <10.1007/978-3-642-39377-8_3>. <hal-01463676>

HAL Id: hal-01463676

https://hal.inria.fr/hal-01463676

Submitted on 9 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Developing Cyber Competition Infrastructure Using the SCRUM Framework

Heath Novak [1], Daniel Likarish[1], Erik Moore[1]
[1]Regis University, Denver CO, U.S.A.
{novak667,dlikaris,emoore}@regis.edu

Abstract
In March 2012, the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC) was hosted at Regis University and attended by seven colleges from the region. CCDC was developed by the University of Texas in San Antonio to provide a structured environment for practical education tied to established information assurance learning objectives in the implementation of security techniques, strategies and processes. The Regis University infrastructure team designed the competition scenario to emulate an e-commerce web business. The pervasiveness of web application attacks resonated with the event developers at Regis University because of recent reported attacks against Valve, Inc. and their Steam video game retail and social networking service. This paper will outline at a high level the event architecture and technical infrastructure details, a discussion on Agile development methodologies (specifically SCRUM) and how they can be applied to competition infrastructure development.

Keywords
Collegiate Cyber Defense Competition, CCDC, Cybersecurity, Information Assurance Curriculum, Agile, SCRUM, SDLC, Capability Maturity Model Integration, CMMI

adfa, p. 1, 2011.
© Springer-Verlag Berlin Heidelberg 2011

1. Introduction

The Collegiate Cyber Defense Competition (CCDC) [10], developed and organized by the University of Texas, San Antonio has steadily grown to encompass all 50 States in the Union. In 2012, Regis University joined the CCDC family by hosting the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC). A total of seven schools participated in the event and six out of the seven teams competed for the chance to be invited to the Nationals competition. Victorious student competitors from all hosted CCDC regional competitions are invited to compete for the top prize at the University of San Antonio Nationals. The last report by an official within the University of San Antonio CCDC steering committee stated that all 50 states are onboard to take part in the competition. These schools have a special motivation to be involved because they can gain recognition for their cyber defense curriculum as well as offer a unique opportunity for students to gain hands-on experience assisting in developing the infrastructure for the competition. By competing in the event, students are offered an additional learning opportunity for personal growth and are provided a venue to demonstrate their business and technical skills to potential employers.

The task of developing the information systems infrastructure is not trivial and takes a great deal of coordination and technical savvy. Black is the color identifier for the team in charge of infrastructure development and maintenance for the event. The skills gained and exercised as a member of the Black Team is unique and well-suited for individuals in a general or security-focused information systems engineering role as necessary skills exercised include systems engineering, project management, systems administration, and software development. This paper reviews the project management methodologies as applied to the goals and situation of the Black Team at the Regis-hosted CCDC event and makes general recommendations based on outcomes.

2. CCDC: The Collegiate Cyber Defense Competition

The CCDC event is typically composed of five primary teams: the competitors (Blue teams), the attackers (Red team), the competition infrastructure engineers (Black team), the Blue team facilitators (White team) and the judges/rules enforcers (Gold team) [10]. The CCDC event typically consists of six Blue teams competing in the event, although the RMCCDC event hosted by Regis University had a seventh non-competing team. Each Blue teams consisted of eight individuals (two graduate and six undergraduate students) tasked with protecting a pre-configured and provided information system infrastructure functionally identical to that of the other teams.

The information system infrastructure consists of flat network architecture, various servers and workstations supporting valid business or mission-critical applications that emulate the internal functions of a real-world organization. Injecting realistic customer, business, and security events into the event enhanced the knowledge gained by the participants to achieve greater real-world value and therefore more benefit later when they enter the workforce.

The scenario touches on current events and includes valid applications that leverage standard Internet protocols and security controls. Further, the scenario includes enough content to keep the competitors busy with deliverables that demand effective communication between team members in order to emphasize the importance of interpersonal communication during periods of critical activity. One key facet of the event is the injection of stress, or "injects," such as providing deadlines for specific business reports and change requirements as written and enforced by the Gold team. These injects are service level agreements (SLAs) that are provided up-front and include specific deadlines for completion, typically within an hour. Injects can also be issued randomly, in order to simulate normal, on-demand business activities. Inject responses allow the Gold Team to assess how the competitors handle normal business activities along with the threat of attack from malicious actors.

3. Background

Regis University previously hosted and developed information systems infrastructure for CANVAS (Computer and Networking Virtualization and Simulation) cyber competition. This initial foray into this realm of cyber competition development offered insight into how to improve the development of infrastructure for future events including consideration of the project management methodologies. The Regis project team developing cyber competitions improved its approach in developing RMCCDC from lessons learned in the development of CANVAS, such as introducing advanced scenarios based on current threats, prevailing security and networking technologies, and improved monitoring capabilities. But the team fell victim to some of the same mistakes and constraints adversely affecting the effectiveness of monitoring and testing coverage. The network topology for the public and private networks designed for the event made it difficult to monitor full Red and Blue Team activities. As a result, a flat, isolated network will be favored for future events. Testing was hampered by severe time constraints caused by late arrival of necessary equipment and Black Team scheduling difficulties. In order to improve the level of capability of the team, efficiency of work, and quality of outcome, the team decided to apply a standard methodology for a systems development life cycle (SDLC). The reason that the team decided this is because it recognized standard artifacts of project dysfunction in the previous work and realized that a more formal approach was necessary to ensure success. Cyber competitions are a type of product, one from which the host can gain value as well as the various participating teams. During our trial and tribulations in building RMCCDC, we realized that cyber competitions exemplify the goals and challenges of Enterprise Architecture; that is to integrate novel approaches in executing in the most efficient and agile way possible, the strategies for developing of the final product. It is therefore quite clear that an appropriate development lifecycle methodology be leveraged for developing cyber competitions.

Based on the above realization, in 2012, the Regis University Black Team implemented a diluted version (i.e. lacking a full set of phases) of an Agile SDLC, where there is somewhat less formality and a greater emphasis on people and their interactions. Although the Agile Methodology is generally specific to software devel-

opment, the same principles can apply to system engineering projects, at least those facets that relate to people and their interactions. Additionally, agile methodologies place strong emphasis on risk management, since projects of any size are rife with risk requiring effective time management, communication and prioritization of tasks. The focus on risk was particularly important to the team because of the need to produce a resilient infrastructure with a volunteer team in a limited time. Extending analysis of these affinities, the next sections present a review of Agile methodologies, and then particularly SCRUM methodologies as applied by the Regis cyber challenge development team along with an evaluation of the change in performance outcomes attributable to the use of the SCRUM methodology.

4. Agile Software Development Methodologies

Initially, the cyber competition development team did not consider using an agile method to drive development of the competition infrastructure; this came about as we were actively working to get the deliverables completed. We realized later into the process that due to the timeframe, scheduling and manpower availability constraints, we couldn't use a traditional software development lifecycle (SDLC) approach. Since we just started taking part in the CCDC circuit and didn't have experience in developing cyber competitions other than CANVAS we chose to embrace, in an ad-hoc way, the ideals set forth in the Agile Manifesto (http://www.agilemanifesto.org). There are many conceptual and practical parallels between software development and information systems infrastructure development, which includes just about every Internet technology engineering discipline. Therefore, we feel confident that using an agile project management methodology greatly improves the final competition deliverable as well as satisfying several academic objectives for students taking part. We assert that using the SCRUM framework, developed by Ken Schwaber and Jeff Sutherland [8], would serve the purposes of the competition host best.

5. SCRUM, An Agile Method

First and foremost, SCRUM is a process *framework*. More specifically, it is an iterative and incremental agile software development method, so again its focus is on managing software development. Yet, there are parallels with software development and information system infrastructure development such that the same core values and mechanisms of the SCRUM framework can be applied to cyber competition infrastructure. As a result, it serves to take a closer look at how we could have leveraged, and leverage more effectively in the future, the SCRUM management framework for development of RMCCDC infrastructure.

The actionable roles in SCRUM consist of SCRUM Masters, Product Owners, and a Development team [7]. A SCRUM Master is very much like a "Project Angel" since they enforce process adherence and protect the development team from disruptions that can cause missed deadlines [7]. There is typically a single Product Owner in the SCRUM framework, a person who is the primary stakeholder. In the case of cyber competitions hosted by schools, the product owner would be the Director of the Computer Information Systems Dept. or pertinent faculty members in charge of meeting

obligations agreed to by the University as a new member of the CCDC family. The Development Team would be the Black Team, which is generally comprised of current Practicum students and former alumni volunteers.

In addition to the different SCRUM roles, the other important facet of SCRUM is the iterative process within the SCRUM framework, specifically a concept referred to as a "Sprint." A Sprint is the "heart" of SCRUM and is in essence a time-box of one month or less in which to get things "Done" [9]. A Sprint is completely agile in nature considering that it directly follows the manifesto by embracing "individuals and interactions over processes and tools" [1]. Sprints contain the following characteristics; 1) change control to protect Sprint goals, 2) Development Team composition remains constant, 3) quality goals do not decrease, and 4) the scope may be clarified and renegotiated between Product Owner and Development Team as issues are discovered [8].

In SCRUM, there is also a concept referred to as a backlog, which defines specific work deliverables that result from the stories defined in the Release Planning phase [8]. Stories are based on use cases, a carryover from traditional software development requirements definitions. Since we are developing cyber competitions, the primary requirement is contingent on the chosen scenario, in this respect a form of use case, since it models something that exists in the information technology industry, such as a for-profit web application or critical infrastructure (e.g. power utility, railway station, prison, etc.).

6. How Ad-Hoc SCRUM was applied to RMCCDC

Our initial requirements phase encapsulated the classic SDLC initial requirements phase: to identify the general requirements for the final product and provide enough detail for the system designers to begin designing the solution. The Product Owner, Regis University, along with the development team decided to raise the bar from what we built for the initial foray into cyber competitions, CANVAS. This time out, we introduced elements drawn from the Open Web Application Security Project (OWASP) Top Ten list of web application attack methods (http://www.owasp.org). Therefore, we knew we wanted to build an infrastructure modeled as closely as possible to a public, for-profit web application as well as the expected supporting systems, such as email server, domain controller, FTP server, etc. that an organization would use to satisfy daily business needs. After identifying a model inspired by a real life hacking incident, the aforementioned Steam™/Valve® hack [6], we decided to emulate this environment for our scenario. The end product was a web application simulation, one that could be attacked by a Red team and protected by a Blue team. The requirements defined by these systems, their respective configurations, and content would be the backlogs that the development team members would work on. We propose that a SCRUM Master (or multiple depending on the size of the project) be assigned to manage the development of specific components of the environment in order to keep progress on track.

We assigned a SCRUM Master to maintain progress on the web application backlog (including the Apache server, PHP code, database, FTP server, etc.), another SCRUM Master managed the network development, and a third SCRUM Master to manage the business support environments; Windows systems that implement common business support functions such as role-based access control (e.g. Active Directory), email services with Exchange 2007, employee workstations, etc.). We assigned SCRUM Masters based on their core competency and interest level within each discrete technology domain (i.e. network, web application, business support servers, etc) in order to maximize effectiveness. However, the size and complexity of the infrastructure will dictate the necessity for multiple SCRUM Masters. The assignment of SCRUM Masters is greatly dependent on the manpower, competency, and interest level on hand since students may not desire a project manager type of role. The scenario requirements outlined for RMCCDC provided enough detail for the designers in the next phase to identify how they would implement the infrastructure in question.

Iteration 0, the phase following the initial requirements phase in the SCRUM process, includes the development of the necessary infrastructure required for the scenario in question. This stage included the acquisition, installation, and configuration of various information systems, including storage area network (SAN) equipment, networking equipment, and virtual infrastructure hosts with various relevant guest operating systems (i.e. Linux and Microsoft Windows) to serve the desired applications. This portion of the development process was not without problems, so the team solved problems as they arose, which necessarily generated a backlog of work that needed to be completed. Due to scheduling issues with our volunteer staff, we utilized email or instant messaging to communicate critical progress or blockers and spaced out our standups to twice a week rather than daily, leveraging Practicum course time for this activity. When necessary, priorities were reset and other important tasks were given favor so that at least some progress would continue. The Product Owner and Development team developed a project plan, network topology diagrams, and system characteristics to be used in the infrastructure. To minimize risk, we pursued the quickest and most cost-effective method to build a working e-commerce web site. We chose Drupal as the web site engine and UberCart as the shopping cart module since they best met our needs at the time. The public-facing web and database servers, along with an IPv6 network, created a sufficiently challenging attack surface for the Blue Teams to protect.

Since CCDC is largely an academic device, the alignment of individual student projects with the development of cyber competition infrastructure is encouraged. For instance, after offering the opportunity to take part in the development, specifically to Practicum participants, it would behoove the Practicum instructor to gather from students their specific areas of interest and/or core competency, so they could be more effectively utilized. After all, a motivated worker is a productive worker. In a sense, we would be “killing multiple birds with one stone,” such that students would get graded work in an area of their specific interest while gaining the valuable skill set of building a functioning information system for a real customer - the competition par-

ticipants. In other words, they gain some measure of startup experience. Various facets of systems engineering and software development are touched on, such as quality assurance, project management, information security, and systems engineering. As we discuss the Development Iterations phase, it should become clear to the reader how the scholastic endeavors of students are served through their involvement in cyber competition infrastructure development.

In the Development Iterations phase, we implemented the required systems using common-off-the-shelf (COTS) software. We installed and verified the minimum operational levels; that the guest operating system in the virtualization environment would successfully boot, that we were able to install applications and that the applications functioned as we would expect. We then introduced and enumerated vulnerabilities for individual components to be mitigated by the Blue Teams, as well as business injects, tasks performed as part of normal business operations, during the competition. We were mindful of feature creep, we didn't want to block good ideas that come late; rather we prioritized based on value or ease of integration. This again should remind us of the facet of SCRUM that allows for continuous re-evaluation and the promotion of effective additions to the product.

The best way to test the competition environment is to put it through dry runs with mock Red and Blue teams (such as the Black team split into two groups) to verify that the environments built for each team functioned as expected. Our experience with CANVAS was such that we literally crammed what should have been four weeks of testing time into one week. We experienced similar problems with RMCCDC, but mostly because of delays in hardware acquisition that pushed critical portions of the infrastructure, in this case the network, into backlog. The late arrival of equipment and delayed implementation of network resources prevented the necessary stress and penetration testing to ensure confidence that the infrastructure would handle the load during the event. It is clear that the testing portion of the implementation phase was not nearly sufficient for a regional cyber competition, much less a national one. However, the infrastructure held up well during the competition thanks in large part to the effective work completed up-front in the design and implementation of the systems infrastructure.

The next phase of RMCCDC, called the Pre-Release phase in SCRUM, include integration of the various infrastructure components (e.g. network, servers, applications). This integration is a crucial piece of the puzzle since it will be what will be released for use during the competition and must be tested to make sure everything works as expected. In other words, final acceptance testing occurs in this phase. Additionally, all documentation will need to be finalized, such as business injects and instructions for the event i.e. access control, printing availability, communications, rules, etc.

The Production phase would be the actual competition itself. We had several problems, mostly with the network, that caused some unnecessary frustration for pret-

ty much everyone. However, strong teamwork and effective troubleshooting saved the day, as we were able to get activities moving pretty quickly after the initial outages. Future cyber competition development must take better care in adhering to each phase of the SDLC, but with a special emphasis on testing and tracking metrics to gauge effectiveness. Agile methodologies, and by extension SCRUM, are quite different from traditional development methodologies in that they favor maximization of return on investment (ROI) rather than satisfaction of requirements [9]. As a result, there are very limited formal metrics or measurements that can be used to track progress or success. In fact, the most formal metric is based on output from SCRUM meetings, short "stand up" sessions that highlight individual efforts. The "stand up" session is meant to stimulate discussion and admission of problems that could affect progress. Stand-ups are also used to discuss progress on "Burn Downs", the term used to define the quantitatively the work remaining in a sprint. SCRUM Masters are expected to perform most of the documentation and performance monitoring since they are not responsible for specific development tasks [2].

7. Capability Maturity Model Integration

There is value in discussing how SCRUM relates to advanced models for information systems development, such as the Capability Maturity Model Integration (CMMI), a product of Carnegie Mellon Institute, is focused on managing continued process improvement in the enterprise. Cyber competition development does not need to reach the higher levels of CMMI, but it is useful to understand how CMMI can relate to this proposal. RMCCDC reached CMMI Level 1, which is basically the same as saying that the final product followed general ad hoc processes. As discussed previously, we recommend reaching a level better than Level 1, since doing so will improve the chances of a successful implementation and maximize the learning potential for students taking part on the Black Team.

Neil Potter of *The Process Group* analyzed how SCRUM and CMMI work together [7]. It turns out that SCRUM, an agile project management framework, fits very well in the first three levels of CMMI. Since our goal with using SCRUM is to improve the successful completion of cyber competition development and to get to the point where it is possible to introduce more sophisticated scenarios, it is obviously useful to be able to speak about performance in CMMI terms. Incidentally, the inclusion of SCRUM and CMMI practices enrich the experience and learning objectives for the Black Team members building the infrastructure.

8. SCRUM and CMMI Mapping

SCRUM does not cover Levels 4 or 5 in CMMI, and for good reason, because doing so would violate the fundamental tenets of agile life cycle development. SCRUM mandates flexibility and a focus on customer needs, which are often in flux throughout a project life cycle. Therefore, it is not desirable to integrate Level 4 and 5 processes because they are often heavy in measurements and documentation. We would not want project management tasks to take away from the already limited time available to build the infrastructure.

Researchers at the Technical University of Madrid have analyzed and mapped the various phases of SCRUM to levels 1, 2, and 3 of CMMI [4]. The researchers used a novel approach that visualizes quite clearly how well SCRUM covers the various goals of CMMI in the early levels. The mapping in Figure 1, as developed by the Madrid researchers, claims to prove that SCRUM is compatible with CMMI for the primary reason that both life cycle approaches are working towards the same goal – a fully functioning product that meets the customers' needs. Neil Potter takes the mapping a bit further by showing clearly how SCRUM maps to an extent in CMMI Level 3 [7]. It is easy to see that introducing SCRUM as the framework for developing cyber competitions also satisfies learning objectives related to project management – a net win for the hosting university.

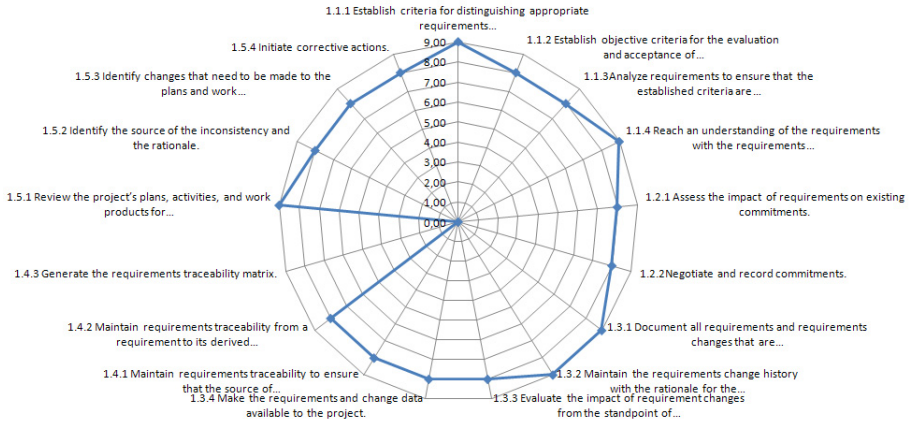

Figure 1 - Managing Requirements (Source: Diaz, Mapping CMMI…, Page 10)

We also recognized that proper risk management goes a long way to weeding out potential blockers or constraints so as to increase the chances of successful project completion. Therefore, risk management must be invoked throughout the development process to minimize loss probability.

9. Risk Management in Cyber Competitions

Risk Identification is generally the first step in risk management, which includes categorizing the potential risks in order to determine which components have the greatest impact on the success or failure of the project [4]. Taken in the context of a cyber competition, an example of a risk would be the choice of network hardware or a specific network design and how it would affect the overall competition experience. For instance, threats such as unavailable network hardware or a poorly designed network would have a negative effect on competition success. Therefore, the network portion of the competition would be a High Risk item, such that several different threats to the network portion of the infrastructure could cause delays in build-out, testing, and dependent tasks (e.g. application development) or cause the final compe-

tition infrastructure to have failures during the event, thereby incurring negative reaction to the competition by all participants involved. A matrix should be used to list out all risks and apply a corresponding score, determined from the loss probability, in order to identify priority.

Risk estimation is used to estimate the probability of potential loss [4]. Using the network example, loss estimation would be severe if the network is being built from scratch and less severe as the time goes by and the network build-out nears stability. Therefore, the network portion of the infrastructure should be prioritized above all other infrastructure components. If possible, the network should be built and maintained in a flat, isolated, constant state in order to minimize the problems just described for future events. Once the network is developed and kept stable, less time will be required for testing and more time can be allocated to other more advanced scenario components.

Risk Evaluation is another facet of the risk management process [4]. The goal of evaluating risk is generally understood in two different approaches; 1) to identify the best response, such as a contingency plan, or 2) to undergo risk aversive action that can lead to either reduction or acceptance [4]. Feasibility analysis also comes in handy during risk evaluation, since it helps to identify facets of the competition scenario that may be too difficult to carry out and are best left out of the event (i.e. risk avoidance). Using SCRUM can ease the risk management process by keeping competition developers in synch with deliverable status during daily standups, allowing the ability to change course without adversely impacting the project.

How did we fare in leveraging risk management in RMCCDC? We were effective in identifying the risks and taking steps to either mitigate them or avoid them altogether. Using the same network example, we recognized that changing the network topology and Internet Protocol addressing schemes each time a competition is developed created risk, so we developed a plan to maintain an isolated network that would be maintained in a constant state, with minimal changes. The network would be leveraged for course projects when it is not used for competitions, thereby minimizing the costs associated with unused resources. This practice also allowed us to maintain knowledge of the state of the environment so we could address emerging problems sooner.

10. Conclusion

There are many benefits to the development and execution of cyber competitions at the collegiate level. They are primarily based on assessing and exercising technical skill in the realm of cybersecurity, but are also effective for students attuned to other information technology disciplines. They offer an unparalleled apparatus for education as well as team and individual skill assessment on technical activities related to system administration, network operations, and software development. How well do team members work together to solve a problem or develop a solution? How well do individual team members handle their respective tasks? These questions can be asked

of Blue Teams as well as Black Teams. The development of cyber competition infrastructure is not a trivial undertaking and requires people skilled in information technologies to design, develop, implement and test the infrastructure. Competition infrastructure development is an excellent learning apparatus, in that multiple facets of information technology are touched upon. Thus, students should take a significant part in developing the competition infrastructure because the exercise offers highly valuable skill development.

Scenario details, the theme for the competition, are very important since it will primarily determine the learning objectives in the competition. It is important to mention that they are not easily used as a gauge for large-scale or global assessment of attack techniques or mitigation capabilities due to scope; the cost of equipment, space, and demands related to network isolation. Realism is paramount, but the scope should be focused on the flavor-of-the-month attacks in order to educate about, or assess relevant skill sets against, current attack methods. CANVAS 2011 focused on Smart Grid security and touched on the Stuxnet phenomenon while RMCCDC 2012 focused a bit more on web application security because they were highlights in their respective time periods.

Traditional SDLC methods do not truly fit the characteristics of developing cyber competition infrastructure at the academic level, because traditional methods are often stringent and heavy on documentation, measurements, and formal meetings. A loose group of students, part-time volunteers, and faculty would not be able to follow such a strict and formal project plan. Therefore, SCRUM is an excellent choice for adoption because it was created to ease the difficulty of managing projects that have tight time schedules, fluid requirements, and limited resources, which are all staple characteristics of cyber competition development. Additionally, SCRUM is growing in popularity in the business world due to its success in improving the effectiveness of project management, so the students and volunteers taking part in developing the competition will gain valuable experience with its use. SCRUM is compatible with the first three levels of CMMI, thereby showing that continuous process improvement can be maintained using SCRUM. Additionally, Risk Management techniques should be leveraged to minimize loss probability of cyber competition components. Using the SCRUM framework for developing cyber competition infrastructure will not only improve the successful deployment but also prepare students for following similar frameworks in their future IT careers.

Bibliography

1 The Agile Manifesto. (2012). *http://www.agilemanifesto.org*

2 Brown, C., DeHayes, D. et al (2009). Methodologies for Custom Software Development. *Managing information technology, 6th edition.* Pearson Prentice Hall. ISBN-10: 0-13-178954-6

3 Carlin, A., Manson, D., Zhu, J. (2010). Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (CCDC). *Information Systems Education Journal, Vol. 8 No. 14*. ISSN: 1545-679X. Retrieved May 1, 2012 from http://isedj.org/8/14/ISEDJ.8(14).Carlin.pdf

4 Coyle, S., Conboy, K. (2009). A case study of risk management in agile systems development. *17th European Conference on Information Systems. http://www.ecis2009.it/papers/ecis2009-0642.pdf*

5 Diaz J., Garbajosa J., Calvo-Manzano J. A. (2009). Mapping cmmi level 2 to scrum practices: an experience report. *EuroSPI 2009, CCIS 42. pp. 93-104*. Retrieved from *www.cin.ufpe.br/~scls/Claudia/INVE_MEM_2009_69756.pdf*

6 Poeter, D. (2011). Valve's steam forums hacked, not clear if credit card number were stolen. *PC Magazine, PCMag.com.* Retrieved March 10, 2012 from http://www.pcmag.com/article2/0,2817,2396246,00.asp

7 Potter, N. (2010). Comparing scrum and cmmi, how they can work together. *The Process Group.* Retrieved from *www.dfw-asee.org/archive/scrum-cmmi-v1p6-45mins.pdf*

8 Pressman, R. (2005). Agile Development. *Software engineering, a practitioner's approach, 6th edition,* (pp. 85-87). McGraw-Hill Series in Computer Science. ISBN: 0-07-285318-2

9 Schwaber, K., Sutherland, J. (2011). *The scrum guide, the definitive guide to scrum: the rules of the game*. Retrieved May 12, 2012 from http://www.scrum.org/storage/scrumguides/SCRUM_Guide.pdf

10 White, G. Ph.D., Williams, D., (2005). Collegiate Cyber Defense Competitions. *The ISSA Journal, October 2005*. Retrieved April 15, 2012 from https://www.issa.org/Library/Journals/2005/October/White,%20Williams%20-%20Collegiate%20Cyber%20Defense%20Competitions.pdf