Communication and Teamwork in a Virtual Learning Environment

Overview
Information security must be understood not only as a technical problem but also as a complex human factors issue. Numerous technical advances in information sciences and cybersecurity do not always produce more secure environments. Computers are operated by people and human factors influence how individuals interact with each other and with information security technology; it is this interaction that is often not addressed in the development of virtual learning environments for students.

Human factors also play a significant role in advancing computer security as verbal skills, listening skills, cognitive abilities and personality traits impact on individual and collective behavior. Behaviors are also influenced by the environment and organizational culture in which they occur. These factors interact with one another and can result in decisions and actions that are often detrimental to information security.

Observations of students working in cyber teams and their progression through the simulations provided important data that allowed for a set of recommendations to emerge, impacting the greater likelihood of success in developing and facilitating student teams in cyberspace. Because the pilot project was iterative, the identification of successful outcomes and the identification of limitations within the experience provided numerous opportunities to share strategies and best practices as well as adjust and modify the scenarios providing greater opportunities for learning and growth.

The Virtual Collaborative Learning Laboratory (VCCLL) and the CyberCorp experience was conceptualized as a project to provide students with real-world cybersecurity simulations; to engage them in the process of learning through experience, and learning through reflection. These simulations provided participants with a form of experiential learning that included students reflecting on their experience of working with cyber teams on a variety of security threats.

There were two aspects of the CyberCorp simulation that were identified as influential toward student learning within the project. The first, focused on the impact of students experiencing real-time scenarios requiring them to work with peers in an imbedded, virtual environment. It was hypothesized that students participating on cyber-teams associated with one of the three companies (Glass Hammer, Carbon Fiber Anvil or Port Hosting Authority) would have to develop their communication skills while working with cyber partners at other locations as they moved through the simulations. The second anticipated impact focused on the nature of the interactions between students co-located at the various physical sites where simulations occurred in large, open lab spaces. While students at each of the three physical sites were assigned to a virtual company with participants at other institutions, the proximity to their fellow students provided the opportunity for considerable cross communications within the physical learning environments. Students co-located in the physical spaces were also learning and assisting one-another. Regardless of their assigned roles as network professionals, students were sharing their experiences in real time, assisting one-another, utilizing their individual strengths and skills as events unfolded and attacks
arose in the simulation. Students assisting one another was not discouraged as long as it did not affect their performance on their own Cyber-teams.

**Observations**

*Student Self-Awareness and Learning*

The observational process included a series of de-briefing conversations with students (at each of the sites) at the end of each full day of Cyber Corp. Several themes emerges from these conversations. Students remarked on their enhanced level of confidence in problem-solving, their increased appreciation working on cyber teams and for some, a renewed confirmation of their academic choice and career path in Information Technology (IT) and Cybersecurity. As importantly, participation in the simulations enabled students to learn how to support and rely on their cyber team members. This reliance included developing and enhancing their communication skills with their team members, and developing strategies in addressing security threats that required following best practices and identified standard operating procedures.

Additionally students expressed an appreciation for participating in the hands-on training simulations while learning about standards and procedures relevant to working in the field of information technology. Beyond the overall experience in the Cyber Corp simulations, students were able to discuss how security issues permeate throughout the IT environment. Upon reflection, many students acknowledged they had preconceived notions of “IT Security” as major events, or attacks on networks, whereas through these simulations they experienced a more realistic IT and security environment.

*Student Engagement and Teamwork*

Developing good virtual teams presents all the same challenges (group dynamics, active listening and oral communication) as in developing face-to-face (f2f) teams. However, the nature of virtual teamwork adds additional complexity; both in terms of needed proficiency among team members to perform and work virtually but also in the degree of personal comfort and trust in working with strangers. In the early stages of the scenarios, some students depended more on their f2f peers who were in physical proximity in the learning lab more often than their virtual counterparts. However, as students became more familiar with each other, their reliance on their cyber counterpart team members increased as the simulations progressed over time.

To be successful, virtual teamwork must address any technological challenges for team members, understand communication protocols for each participant on the team, as well as address connectivity issues and communication challenges. An example of communication issues in the CyberCorp simulations occurred when mobile phones were adopted as a means of peer-to-peer communication as signal strength declined within the interior of closed spaces. In some cases, students had to leave their stations to call members on their team in order to complete some of the tasks. Eventually, this issue led to the development and adoption of better and alternative communication strategies within teams in addressing this and similar collaboration challenges.

*Facilitators and Cyber-team Preparation*
Providing additional learning opportunities for students before entering the virtual Cyber Corp experience can strengthen their ability to engage with peers and maximize benefit from team interaction and collaborative work. Observational data gathered during the Cyber Corp simulations clearly support the importance of pre-work in the areas of team-building and the strengthening of communication and listening skills as much as technical skills development. Special attention should also be given to the unique nature of team effort and team relationships in virtual environments. Pre-work should also be augmented by additional emphasis on community building with either an f2f or virtual launching event prior to the start of simulations where team members are introduced to one another and given an opportunity to interact and socialize.

The role of the facilitator is key in providing a sense of direction to students regarding the overall experience and ensuring that all student team members, participating faculty and staff and external participants at each site are clear as to the desired outcomes of the events. Reference materials (facilitator and participant guides) were developed that addressed job descriptions, company profiles, and standard operating procedures. These documents were a valuable aid in working to resolve confusion that often emerged about individual roles and responsibilities. Additionally, facilitators must be able to provide students entering the scenarios with a good working knowledgeable of the simulation’s environment at both a “normal” and “disrupted” state.

Scenario Facilitation

Scenario facilitators must be skilled as technology guides. However, facilitators of virtual teams face additional challenges in coordinating virtual teams. For many of the student Cyber Corp team members, the online interaction was a new experience. Participants contend with learning the IT environment as well as communicating within the simulation with their respective team members. In developing scenarios and in recruiting and selecting student participants, facilitators must be sensitive to the fact that the learning curve may become too steep for some participants with limited abilities to use and learn complex network tools. Facilitators cannot assume that all student participants are capable of using all of the communication technologies adopted, or that they have a strong familiarity of the network tools adopted in the simulation. A good practice for ensuring there is access to learning resources is to provide or create illustrated 'How to' documents or videos for using all the tools to demonstrate members. An alternative means to this maybe access to online tutorials can be held outside the simulation to provide a discussion area to collectively explore new tools, share best practices, or experiences.

Scenario facilitation requires active and engaged effort on the part of the individual(s) identified to direct the scenarios. These efforts may include modeling and encouraging better communication within the team, directly encouraging team member participation by asking about their responsibilities and involvement and asking student participants to share their thoughts and questions are all important strategies to encourage full participation. Facilitation can take many paths and often reflects team dynamics, the individual approaches of faculty and staff as well as the communication preferences of students.
Finally, facilitators need to be aware that one member’s communication can influence others. A good tool for facilitators is process checking. By engaging the team and probing to inquire whether, “Is the purpose still clear? Is our approach working? Are we making progress? Is the pace of the tasks at hand ok? Have we lost anyone in the progress?” When communications between members moves off-track or possibly moves toward conflict, facilitators can intervene and clarify and interpret discussions, or keep team members on track by a restatement of goals and objectives to remind them of their purpose within the simulation.

*Facilitator Cyber-Team Limitations and Challenges*

Determining the facilitative process requires a number of choices such as the styles of interaction, the management of group dynamics and the working climate. In general, students who participated in the Cyber Corp scenarios possessed relatively equal skills, however, observational data gathered during the simulation events suggested that in some cases, students who had some previous training, work experience, or higher-level course work completion were more engaged in the simulations than students with little to no previous exposure. As an iterative process, many of the instructional and operational aspects of the scenarios were changed as the team and facilitators explored the event and shared reactions and insights about the experience. As an example, in the first Cyber Corp scenario, cyber teams were assigned (randomly) to specific organizational positions with minimal explanations of job duties or standard operation procedures for specific positions. Students were unclear as to their roles and that lack of clarity impacted the outcomes of the early scenarios. That early experience of our students within teams (communicated during debriefings) led to the development of more extensive job descriptions and the refinement of assignments and expectations.

Lastly, beyond the challenges of any team leader, there are unique aspects to leading virtual teams (especially students) including individual pressure upon and reluctance to interact and work with others within cyberspace rather than face-to-face environments. Cyberspace produces extraordinary conditions that are created when people interact with computers and networks at a metacognitive level, in the creation of a psychological "space." When people access computers, launch programs, create e-mails, or log on to online services, users often feel - consciously or subconsciously - that they are entering a "place" or "space" that is filled with an assortment of meanings and purposes. How people behave in cyberspace will always be a complex interaction between these features of cyberspace and the personality characteristics of the individual. These personal psychological “spaces” are additional conditions of the cyber-team’s work environments to contend with internally and evaluate externally.