Journal of Information Systems Education

Volume 32
Issue 1
Winter 2021

Collective Learning for Developing Cyber Defense Consciousness: An Activity System Analysis

Melissa Gross and Shuyuan M. Ho

Recommended Citation: Gross, M., & Ho, S. M. (2021). Collective Learning for Developing Cyber Defense Consciousness: An Activity System Analysis. *Journal of Information Systems Education*, 32(1), 65-76.

Article Link: https://jise.org/Volume32/n1/JISE2021v32n1pp65-76.html

Initial Submission:	8 June 2020
Accepted:	1 September 2020
Abstract Posted Online:	10 December 2020
Published:	15 March 2021

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Collective Learning for Developing Cyber Defense Consciousness: An Activity System Analysis

Melissa Gross
Shuyuan M. Ho
School of Information
Florida State University
Tallahassee, FL 32306, USA
mgross@fsu.edu, smho@fsu.edu

ABSTRACT

This paper explores the perceptions of undergraduate students experiencing an educational intervention in a cybersecurity course. The intervention was developed using activity theory. Laboratory activities were designed to 'protect' and 'poke around' systems and networks in a sandbox cloud environment. These activities provided dynamic opportunities to tackle cyber challenges through teamwork. Transcripts of interviews with students (working as system administrators) were analyzed to describe the development of their cyber defense consciousness. Activity system node analysis reveals the transformative development of cybersecurity consciousness over time that involves the internalization of skills and knowledge; reliance on community for support, information, and acculturation; working with others through the division of labor; as well as their struggle with the demands of cybersecurity work. The cyber defense activity model further unveils the potential of collective learning in teams as depicted by four mediated relationships. The study contributes by building a foundation for a pedagogical approach that transforms the cyber defense consciousness through the collective learning activity model.

Keywords: Cybersecurity, IS education research, Team-based learning, Experiential learning & education, Qualitative research & analysis

1. INTRODUCTION

The importance of cybersecurity in the digital age cannot be overstated. The difficulty of cyber defense also cannot be overstated. Data breaches and hacking attempts are frequently in the news. At the time of this writing, concerns over attempts to steal intellectual property related to the development of treatments and vaccines for coronavirus illustrate the high stakes of data security (BBC, 2020; Wall Street Journal, 2020). In addition, the 2019 Data Breach Investigations Report (Verizon, 2019a) reveals that the main motivation for attacks is financial (71%) and that espionage accounts for 25 percent of attacks. Verizon states that "No organization is too large or too small to fall victim to a data breach. No industry vertical is immune to attack. Regardless of the type or amount of your organizations' data, there is someone out there who is trying to steal it" (Version, 2019b, p. 2). Defending against these bad actors is increasingly complex, and the complexity increases as new technologies (cloud-based solutions, payment card applications, phishing on mobile devices) proliferate. Attackers and defenders can be seen as engaged in a serious game of chess or a deadly dance in which the same mechanisms that are meant to protect data can be turned into weapons, communication platforms are subject to phishing and fraud, and the interconnectedness of cyberspace means that traceable evidence of everyone's activities can be found. Defending systems against multilayers of cyber threats is a complex objective as attacks come from a variety of directions, and the technology for both defense and attack are constantly changing.

Another important aspect of the current state of cybersecurity is the shortage of qualified cybersecurity professionals (Fulton, Lawrence, and Clouse, 2013; Dawson and Thomson, 2018; Crumpler and Lewis, 2019). It has been estimated that globally this workforce shortage will result in 1.8 million open positions by 2022 (Crumpler and Lewis, 2019). Employers scramble to find job candidates who have the needed "technical skills, domain knowledge, and social intelligence" but who are also "reliable, trustworthy, and resilient" (Dawson and Thomson, 2018). There is evidence that cybersecurity education and training programs are not preparing students to meet the needs of organizations (Crumpler and Lewis, 2019).

How to best train students for a career in cybersecurity remains an open question. Universities are aware of the intense demand for cybersecurity professionals as well a need for a consciousness of cybersecurity in the populous generally as the weakest link is often human behavior (Topham et al., 2016; Dawson and Thomson, 2018). Approaches to teaching cybersecurity have been criticized as being too focused on theory, policy, and compliance audits rather than on technical and soft skills (Crumpler and Lewis, 2019). Many educational approaches have been implemented including case studies (Schneider, 2013), laboratory simulations (Topham et al.,

2016), competitions, gamification, and virtual and augmented reality (Bodea, Dascalu, and Cazacu, 2019). Schneider (2013) suggests that part of the problem is a lack of input into curriculum development by needed relevant stakeholders, but the debate over what should be taught is far from resolved. Suggested curriculums and skillsets have been offered by cybersecurity professionals (Fulton, Lawrence, and Clouse, 2013), the military (Dawson and Thomson, 2018), and the Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) (Topi, 2019), among others.

In this landscape, the development of a consciousness of cyber defense has become vital at every level of society. The concern of this paper however is to explore the perceptions of undergraduate students experiencing an educational intervention in a cybersecurity course. The intervention was developed using the framework of activity theory, and transcripts of interviews with students were analyzed to organize and describe their developing cyber defense consciousness. The research question guiding this intervention is: *Can activity system analysis of an educational intervention reveal the developmental transformation of collective learning in cyber defense*?

The outline of this paper is structured as follows: section two sketches out the study framework by providing a brief history of activity theory, its development as a theory of learning, its adoption by information science, and how an analysis of a cybersecurity teaching intervention can be expressed through activity theory. Section three describes the methods, including research design, data collection, and laboratory activities as a learning intervention, along with the qualitative data analysis. Section four interprets the findings of the activity system node analysis where six components of the activity system provide a rich description of the learning intervention within the framework depicting the development of cyber defense consciousness. Section five further delineates four mediated relationships in each triad of the activity theory model to expand on how the intervention operates to increase students' cyber defense consciousness. Section six presents the conclusions and a discussion of the contribution of this work to cybersecurity education.

2. STUDY FRAMEWORK: LEARNING ACTIVITY SYSTEMS

Activity theory has been widely used and promoted in information science as a framework for investigating the structure, development, and social context of information systems, as well as endorsed as a qualitative data analysis method (Nardi, 1996; Spasser, 1999; Allen, Karanasios, and Slaova, 2011; Iyamu and Shaanika, 2019). Unlike other theories, which are aimed at prediction, activity theory is descriptive (Nardi, 1996), and its theoretical origins see learning as a developmental process that has the potential to lead to transformations in the subject, at the individual and collective levels, as well as transformations in the activities they engage in and the objects they seek (Engeström, 2019).

The development of activity theory in the domain of psychology began with the work of Vygotsky and his students Leont'ev and Luria in the early 20th century (Kuutti, 1996). Vygotsky was a Russian psychologist who was among those who understood learning as a type of human development inherently shaped by history and culture and separate from the process of physical maturation (Cole and Engeström, 1993, 2001). Some of Vygotsky's important contributions were pointing out that learning is mediated through social interaction and that mediating artifacts can be both technical tools and psychological tools, such as language and numbers (Engeström, 2019). The artifact contains elements of history and culture that affect how the subject proceeds and the transformation of the subject through the activity (Cole and Engeström, 1993, 2001). The subject can also have a transforming effect on the artifact and the object of the activity. In 1930, Vygotsky introduced the triad of subject/activity/object as a graphical representation of these ideas, but his interest remained focused on the development of the individual (Engeström, 2019). He was not able to fully realize all of his ideas before he died in 1934 (Cole et. al., 1978). This left activity theory open to be worked on and expanded by others.

Leont'ev was the next theorist to add substantively to Vygotsky's thinking by enlarging the scope from the individual to the collective (Engeström, 2019). He introduced the concept of the division of labor to describe how the collective can effectively pursue an object when individuals take up a range of actions (these constitute the activity) in support of the goal. In this way, he described an object-oriented, artifact-mediated, collective activity system that acknowledges that in addition to technical and psychological tools, people can also mediate objects. Leont'ev did not further add to the graphical activity system model (Engeström, 2019).

Although many others have worked on activity theory, Engeström provided an integrated activity model that incorporates three activity triads: subject, artifact, and object; subject, community, and rules; and community, division of labor, and object that is useful for studying human behavior (see Figure 2 in section 4.1 below) (Cole and Engeström, 1993, 2001). Beginning in the 1990s, researchers working in information science (IS) and the specialty of human-computer interaction became interested in using activity theory for system analysis, system design and development, as a research tool, and as an area of theory to be explored and potentially expanded. This resulted in the publication of *Context and Consciousness* (Nardi, 1996) which brought together a variety of collaborators' takes on what activity theory is, how it differs from other theories, and what it has to offer the field. In 1999, Spasser continued the argument for the use of activity theory in IS, and interest in activity theory is still being promoted in the field as is evidenced by Iyamu and Shaanika's recent work (2019).

While many uses of activity theory have been reported, Vygotsky's focus was on learning. Engeström has stayed true to this idea by using the activity theory model he developed to describe his theory of expansive learning. It is the idea that learning is an activity that can be analyzed that underlies the analysis reported here. The theory of expansive learning is a process that erupts from a set of contradictions that are overcome as abstract concepts become concrete by being expressed as practice (Engeström, 2019).

Cyber defense is an activity that is highly prized by society and yet contains several inherent contradictions that the learner must assimilate. For example, learning takes place in a context in which mastery of the content is a moving target. All that

needs to be known cannot be known due to an increasingly complex set of problems that continue to arise in a landscape of the proliferation of technologies and human ingenuity. Further, while it is important to learn about existing systems and mechanisms, reliance on learned procedures can be a future trap if these tools are privileged over emerging products and procedures that are more effective. This is the starting point of this analysis which employs the method Engeström (2019) called formative intervention. The process of the intervention, in the form of a laboratory assignment, offers students a variety of tools but leaves it to them to negotiate the content and processes within a team structure and for themselves as individual learners. The key outcome that the process seeks is the development of agency – the ability to make decisions and act informed by knowledge and skill – such that students come to see themselves as prepared and able to participate in cyber defense. The instructor's role was to provide an environment within which the expansive learning process would be determined and owned by the students in the class.

3. METHOD

An experiential cyber defense learning opportunity was created during the Advanced Cybersecurity class offered at Florida State University in Spring 2017. Participants were assigned to protect their information assets and networks while responding to computer incidents/emergencies and performing triage in a coordinated manner. Semi-structured, one-hour interviews were performed with students enrolled in a cybersecurity class. The one-hour interview took place near the beginning of the semester as students took on the role of a system administrator. The class had an enrollment of 18, and 15 students agreed to participate in the study. Before subject recruitment, the study was approved by the Florida State University Human Subjects Committee and obtained the Institutional Review Board (IRB) protocols. One student was female; the rest were males. Interviews with the 15 students took place as students were beginning a semester-long, hands-on laboratory project that teaches both defensive and offensive skills. In these interviews, students were asked to respond to interview questions from the point of view of a system administrator. The interview questions were structured to address the six elements/nodes in the activity theory model (i.e., subject, activity, object, rules, community, and division of labor). All interviews were digitally recorded and then transcribed for analysis. One interview resulted in an incomplete transcript due to issues with the recording quality and two of the recordings were corrupted and could not be transcribed. A second, one-hour interview took place at the end of the semester after students took on the role of penetration testers and will be reported elsewhere.

3.1 Laboratory Activities

Students were organized into four teams of four to five students in order to gain experience with security tools designed to protect their web server (they worked with either a Windows Apache 2.2 server or a WordPress on Lamp Ubuntu 12.02.1 server) and workstations. The security tools included defensive tools (e.g., pfSense and Palo Alto Networks Firewalls) and intrusion detection monitors, such as Security Onion and HoneyBot, and penetration tools such as Kali Linux. The Microsoft Hyper-V Management system was the lab platform used to simulate a real-world cloud environment.

The laboratory activities for each team of students included protecting their information assets (including various information systems, tools, and their networks as built and configured behind each teams' assigned firewalls) while performing reconnaissance and penetrating other teams' information assets. The teams' first learning experience was to set up their web servers, workstations, firewalls, intrusion detection systems, honeypots, and network environments. Team members then took on the roles of system administrators who were tasked with system defense. Figure 1 illustrates the expected network topology for each team. Once their systems were configured, team members also took on the roles of penetration testers to exploit other competing teams' information assets using exploitation tools (such as Kali Linux and other techniques) to penetrate other systems and networks. Students were encouraged to be entrepreneurial and to take initiative in troubleshooting their system and network environments to demonstrate both defensive and offensive skills.

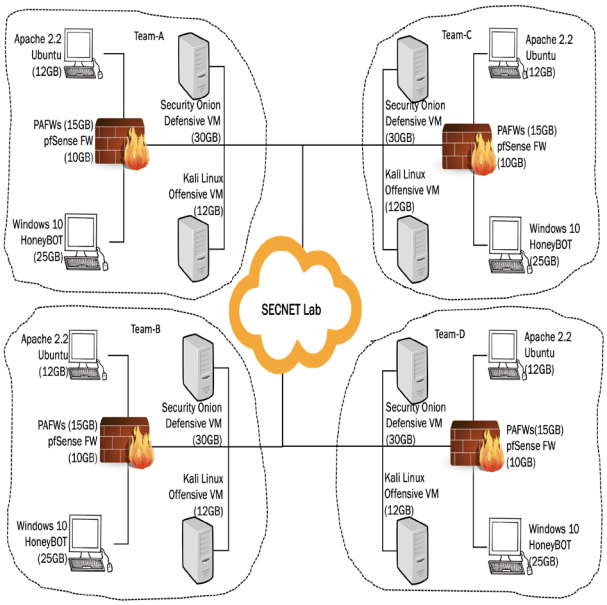

Figure 1. Research Design – Cyber Exercises Conducted in the Hyper-V Environment Hosted on the SECNET Server

3.2 Data Analysis

Transcripts of the interviews were uploaded to NVivo 12, and an initial coding scheme based on the elements of the activity theory model was employed by the researchers. In an iterative cycle, both researchers coded a transcript, and a test of inter-coder reliability (Kappa) was performed. The researchers then met to compare their coding and to discuss the addition of new codes based on the themes that were developing in the data. Discussion of the coding improved the Kappa scores to a range of 0.72 (fair to good) to 0.93 (excellent). Discrepancies in coding were not due to a lack of agreement between the coders, but rather due to differences in the extensiveness of the coding.

To ensure that coding was as extensive as possible, both researchers continued to work together to code all transcripts, agree on the addition of new codes, and review each other's coding. The coded transcripts were then analyzed in NVivo 12.

4. ACQUISITION OF CYBER DEFENSE CONSCIOUSNESS: NODE ANALYSIS

Participants gain cyber defense consciousness through engaging in a series of defense and offense scenario-based activities that are performed individually as well as collectively. Findings in the activity analysis are arranged around the nodes as configured in the activity theory model (Figure 2). The analysis begins with the subject as it is the subject's motivation toward an objective within a social context that allows for the exploration of development in activity theory.

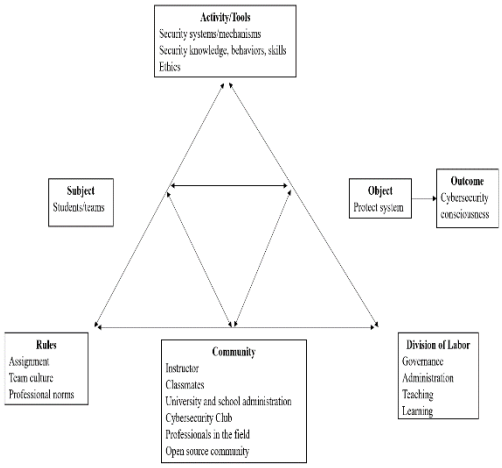

Figure 2. Learning Cyber Defense Activity Model (after Engeström, 2019)

4.1 Subject

The idea of a subject can refer to individuals or groups. In the case of the cyber defense class intervention, the unit of analysis is the individual student, but as the assignment dictated, these students operated within a team structure. The effect of the team on the development of these individuals is important as cyber defense in the workplace is normally a collective activity, and negotiating relationships in order to maintain system security is one kind of expertise that is needed.

Students in the cybersecurity class had varying levels of previous knowledge and experience with information technology. Although all but two were in their senior year, six of the students had only a minimal technical background. These inexperienced students reported being confused, feeling the subject matter was difficult, and lacking self-confidence about their technical knowledge. In comparison, other students had a substantial background on which new learning could rest. For example, one student had an Associate's degree, a CIW certificate, and IT training in the military. Another student had completed two other cybersecurity courses the previous semester, and other students reported learning something about cybersecurity in the context of internships or employment.

Students with different skillsets were placed in one of four teams to complete the laboratory assignment. At the time of the interviews, some of the teams were struggling with their collaboration. There were difficulties agreeing on when and how to communicate outside of class and difficulties organizing and assigning roles. Some students were perceived by members of their team as unmotivated and not pulling their weight. In one case, this had a unifying effect on the rest of the team. As one student described,

> He didn't want to do anything, we knew it, we saw it …and the two other guys they knew it as well, they were always there and made sure it was that one person that stuck out, it was already too late to kick him out of the group. (Student H)

Despite these difficulties, teams described being able to coordinate their work. They began to rely on each other to overcome difficulties and complete tasks. As one student put it, "We were all trying to help each other out because we all wanted to learn as much as possible" (Student M).

4.2 Activity/Tools

Activity is the mediating factor between the subject and the object (Engeström, Miettinen, and Punamäki, 1999). It is comprised of the actions that subjects take to triage and reach a goal, and these actions are determined by motivations and intentions (Nardi, 1996). Because an activity is engaged in to achieve an objective, the activity itself is determined by the objective, motivation, and purpose of the subject as well as the environment in which the activity takes place. If any of these changes, the activity is subject to change as well (Nardi, 1996). Activities can be performed by individuals or through cooperative actions where people are working toward the same goal, giving the activity its shape and sense (Iyamu and Shaanika, 2019). The dynamic nature of the activity is very apparent in the cybersecurity environment where conditions are subject to change almost continuously even as the objective – to defend the system – remains constant.

Within the construct of the laboratory assignment, the activities that the students are engaged in can be broadly understood as protecting their system while penetrating other teams' systems. Engaging fruitfully in these activities requires being able to use a variety of tools. This means developing skills with technology and requires learning new terms and concepts as well as new ways of thinking. As a skill is learned, the external tool becomes internalized, which makes actions more automatic, but also allows an action to be worked out conceptually as it is performed (Kaptelinin, 1996). A typical example of the internalization process is learning to drive a car with a stick shift. At first, the driver has to be very conscious of when the clutch is released and when to change gears. An experienced driver can do this without much thought and can anticipate what will be needed to start driving on a steep incline or to use the gears to slow the car down without using the brakes.

In the cybersecurity laboratory assignment, teams are asked to install and configure systems that included Apache 2.2 Web, pfSense, Palo Alto Networks firewall, Comodo, HoneyBot, Kali Linux, and Security Onion. However, in securing their systems and attacking other teams' systems, they studied and

experienced various threats that they must research and be able to respond to. The Appendix displays the wide variety of tools the students discussed becoming aware of, learning, and using in class. There is a total of nine categories of domain knowledge acquired by students as tools and activities. An interesting discovery is, that in addition to the range and scope of knowledge regarding malware, passwords, database, systems, servers, networks, and physical security identified as important tools, students also recognized laws and policy, virtualization, personnel security, and training as being salient tools to defend information assets.

It is not possible to know from the transcripts to what extent students were able to internalize their use of specific tools during the course, but the movement toward internalization speaks to the developmental dimension of activity theory. It is clear that a wide variety of skill levels existed among these students from the beginning of the assignment, but also that skills are being acquired and strengthened through engagement with the lab assignment. The changing individual skill levels impact what tools are utilized and the sophistication with which teams defend their systems and attack the other teams over the course of the semester. The transcripts make clear that the students have had wide exposure to a variety of tools and concepts that they see as critical to know.

The transcripts also reveal a variety of internalizations of security and system defense concepts. Specifically, cyber defense consciousness is gained through the following themes that emerged and were conceptualized as follows.

4.2.1 Knowledge transfer. Codified (or explicit) knowledge obtained from the textbook is converted internally to tacit (or implicit) knowledge when applied in organizational contexts and based on changing conditions. Internalized knowledge about what must be done to secure a system or network includes the need for correct set-up and back-up procedures; system and software maintenance concerns and procedures; and monitoring procedures using log reports, scanning, and other tools to detect and address malicious software, viruses, and other anomalies. The students also articulated how they would proceed if attacked, such as taking the website, webserver, system, or network off-line and performing various kinds of analysis to detect and fix the problem using back-ups. They also discussed specific safety habits that are important, such as "being smart with passwords" (Student B) and "If you do not personally or professionally know the sender, do not click it" (Student G). One student said, "Just common-sense measures are usually ninety-nine percent of the problem" (Student C).

4.2.2 Think like your enemy. One view of best defense practices was the idea that a good defense strategy is to consider systems from the point of view of a hacker or a "bad guy" rather than from a defensive stance. They asked questions like, what would a hacker be looking for and made comments like "you have to think in their shoes and how if I looked at outside looking in what would be beneficial to me" (Student K) and "You don't wait until someone is actively attacking you" (Student G). Their internalized strategies are proactive, rather than reactive to system breaches. They describe the stance as a "kind of an ongoing process; you have to have a lot of commitment to be in that position" (Student I). Another internalization in terms of tools was the understanding that some tools are a "double-edged sword" (Student E) in that some tools can facilitate both defense and attack depending on how they are used.

4.2.3 Ethics. Primary among the ethical concerns that students voiced was their awareness of issues related to surveillance and privacy. While law, policy, and procedure were cited, more affecting for them were revelations that private files could be made accessible and that students would cheat in completing school work. These ideas upset their sensibilities. Students demonstrated empathy saying "It is like you are going into somebody's house without asking. It is just wrong" (Student H). Student's also had empathy with the other teams by demonstrating a reluctance to crack into their computers and relief over the mandate that they do not use what they were learning for illegal purposes. One student said, "I thought that was a good thing. It was a good disclaimer and every person that was sort of doing all this hacking was in the sandbox environment" (Student L).

4.3 Objects

As Nardi (1996) points out, the object is important because it directly affects the activities that take place. For this reason, there is a reciprocal relationship between objects and activities. If the object changes, this can affect the type of activity undertaken. The nature of the activity in this case was a class assignment, which meant that overall the goals were stable. While students' personal goals may vary, the imposed need to defend their system/network and complete the assignment are predictable and student comments reflected this. For example, they described their goals as "to defend the network" (Student L), "not to be attacked" (Student K), and "to set up a network that was secure" (Student M).

However, from a personal standpoint, the students took very seriously their goal of learning how to be able to protect systems and networks, which was also the purpose of the assignment. This motivation often led them to seek sources outside of those assigned as classwork and in that way expanded both the activity related to learning, but also the activities that comprise protecting their systems and penetrating the systems set up by other teams. The main themes that emerged from the students' descriptions of their information behaviors related to cybersecurity were: the use of other people (see the community section below) and research outside of class they did on their own. They said things like "Most of the time I just do like outside stuff on my own, reading on my own to kind of understand how some things work" (Student I) and "I probably looked at five or six forums that help me out with the defense part of the project" (student L).

Learning was important not only to do well in class, but to attain their long-term objective of preparing for a career in network security, security analysis, or systems administration. As one student expressed it, "Everything uses a computer, so it is going to be one of the biggest jobs out there in a while, it is not even in a while, and it is now" (Student L).

4.4 Rules

The classroom environment and the assignment instructions are the starting point for the rules students are accultured to as they engage in cybersecurity activities. Rules, standards of behavior, best practices, as well as awareness of policy and procedures

that are common in the field of cybersecurity, govern the activities students undertake in completing their assignment. Students are acculturated to these norms through direct instruction in class as well as from interaction with the larger community as described below.

4.4.1 Classroom environment and assignment instructions. Understandably, students were very concerned about adhering to the assignment instructions which mandated the use of certain tools, paper and presentation requirements, due dates, etc., but also left it to them to decide what other tools they wanted to learn and how to best defend their system. Students talked about the need to follow the instructions, and there was a general understanding that the professor "likes things by the book, and if you are not on the book, she doesn't like it" (Student C). It was also made clear in class that although students would be attacking each other's systems, "don't actually go and do some of these things" (Student A). "Everything was on the table for attacks and defenses, but the unwritten rule is for regarding the debriefing afterwards" (Student M).

Some students were so concerned about meeting the requirements of the assignment that they asserted themselves in leadership positions to ensure that instructions were followed completely. This is further discussed under the division of labor below. One student indicated that policies are transmitted in the general community by word of mouth and by talking to other people about your project.

4.4.2 Team rules. Rules of behavior were also developed within the individual teams as they learned to work together. Some of these rules were "don't steal what someone else has done and I guess don't copy someone else's setup, do it on your own" (Student A), "We don't tell anybody what we are doing and we don't want to disclose that information, we keep everything in house" (Student K), and "our best defense is going to an offense attack before we can be attacked" (Student C).

Conflict and competition were only observed twice in the transcripts. The culture of the class was set by the instructor who emphasized the importance of teamwork and who used the concept of "coopetition" to mediate and motivate students in the collective learning environment. None-the-less, when a student took advantage of his unsuspecting peers by changing their Windows passwords and locking them all out of their systems, this made a big impression on the students about how they should treat each other and what happens when people break the rules in a mean way. The other instance of conflict happened when one member of the team wanted to assert himself as the leader but was shut out by his teammates who continued to manage his contributions to the group throughout the project.

4.5 Community

The community node of the activity theory model describes the larger social group(s) to which the subject belongs. These are people who share the subject's goals and who the subject identifies with in terms of the activity in which they are engaged (Iyamu and Shaanika, 2019). A community may be comprised of more than one network or group.

At its most basic level, the immediate community these individuals and teams belonged to was comprised of their instructor and the other students in the class. Other communities invested in their learning include their program of study, school, college, and university. However, the students in the cybersecurity class identified with communities both within and outside of the university. The community within the university was relegated to interactions with people related to their program of study. These people and groups share and support the acquisition of cybersecurity knowledge and skills. These are often people students go to for information or support. At the most informal level, these are fellow students, classmates, friends, and their instructor. One student summed it up this way, "Everyone knows something that you don't, once everyone starts sharing with you, you start bouncing ideas off each other, you start testing what software can actually do" (Student F).

Teamwork and collaboration are recognized as valuable. Student comments include: "I mean I'm trying to make as many friends as possible" (Student A), "In the real world, teams is [sic] how problems get solved" (Student D), and "Dr. Ho, she is all about that teamwork" (Student D).

Another important source of information and support is the Cybersecurity Club at Florida State University (https://cybersecurity.fsu.edu/club/). The Cybersecurity Club is open to all students at the university, and there is no class or program requirement that students join or participate in this club. However, it is clear from the data that several students in the class were participants. The Cybersecurity Club hosts weekly meetings where topical presentations, workshops, and capture the flag (CTF) events take place. The club also competes in the National Collegiate Cyber Defense Competition (CCDC) and hosts informal question and answer sessions on Saturdays. Students describe the Cybersecurity Club as a context in which to learn and hone skills. One student described the club this way: "If you just want to learn about security or technology in a sense, that is a good place to start because they welcome everybody. They have like different projects everybody can work on, it doesn't matter your level of expertise" (Student I).

Contacts from other aspects of life that exist outside of the university (e.g., through internships) are important networks that support these students' progress. Just as students understand the importance of collaboration and teamwork to do well within their program, they also understand the importance of maintaining connections with people who have been helpful to their learning. People they cite as being important and relationships they continue to nurture include family members, connections from high school, supervisors and co-workers from internships or work experiences, contacts from the military or private industry, and contacts made through the Cybersecurity Club such as alumni who serve as guest speakers and representatives of ReliaQuest (https://www.reliaquest.com/), a computer security firm that has provided workshops and support for the club's participation in competitions. One student described interactions with these networks this way:

> When I reach out to my buddies or associates that I have met, I do converse with them about what their daily tasks are because there are so many different views. It is so big, even if you say information security, there is still so much to it. So, I ask them what they do, how

> their organization are [sic] and stuff like that. (Student E)

A final set of networks that are important to these students can be called the open-source community. Information, advice, and opinions are sought online through various websites, mainly Spiceworks (https://www.spiceworks.com/) and StackExchange (https://stackexchange.com/), although students also report using Google to find information: "I'm sure that if I have a certain question that one of my peers couldn't give me the answer to right away, then I would throw it in there and let the online community try to steer me in the right direction" (Student F).

4.6 Division of Labor

As is commonly perceived, division of labor is about not everyone doing the same job in pursuit of a shared objective. The division of labor is expressed in terms of the community. For example, the university, college, and school administration play different roles than the faculty and staff do in supporting student learning. An analogous example of this is provided by Bellamy in the activity she calls K-12 education, where she identifies the community as "teachers, administrators, parents, student, etc." and the division of labor as "principal, governing body, teaching specialist, teaching, learning, etc." (1996, p. 126). In the learning cyber defense activity model, this larger community, which includes the Cybersecurity Club, professionals in the field, and the open-source community, has an interest in the development of these students and performs various roles toward that end. However, of particular interest here is how the students within their teams in their effort to protect their systems handled the division of labor in terms of the roles they took on, the power or status they exercised, and the responsibilities they accepted in support of the objective of defending their system.

Except for the expectation that students would be involved in both defense and penetration testing, the specific roles they assumed within their teams were not dictated by the assignment. This meant that within the individual teams, students had to organize and coordinate their activities themselves, and the teams approached this in several ways. For example, of the 13 interview participants, 6 claimed their group did not have a designated leader, 1 claimed co-leadership with another team member, and 6 claimed that they were their team's leader. As there were 18 students in the class and only 4 teams, it is clear that respondents' experience of group leadership tended to be subjective. None of the respondents reported team discussions about assigning formal leadership roles. Of those individuals who saw themselves as team leaders, they felt they performed this role because they took more initiative, were able to organize the work and make sure tasks were completed on time, or had previous experience that others on their team lacked.

All of these team leaders, including the co-leaders, appear to have assumed themselves into these roles. Data on who was in which group is not available, but one student said, "I think I just took charge" (Student K) and another described the selection of the leader as "He just took over and we were all willing to let him" (Student M). In another case, a student wanted to be the team leader but was not accepted in this role by the group: "There was one individual who tried to assert himself as the leader, I think it was five people and four out of five of us were like, no" (Student H).

For the majority of people who saw themselves as the leader, their role was not official. While individuals felt like the leader of their group, it appears that some groups did not realize that they had a leader and also that more than one person in a group may have considered themselves to be in that role.

One of the main traits exhibited by these "leaders" was a strong sense of responsibility for getting the work done and making sure it was done correctly. They talked about assigning roles among the members of their team, reminding team members about what they needed to do, keeping their attention on due dates, and interacting with the professor to clarify expectations and actions on the team's behalf.

> I made sure that my group understood what was needed and yeah, I stepped back and I let people do what they wanted to do but at the same time I made sure that everything was followed. Everything was on point that needed to be done, so I did a lot of the checks and balances on the side, so I would tell my teammates, make sure that we did this and did that. (Student H)

Technical expertise was also a reason why individuals self-identified as the team leader, and technical expertise was how teams decided who did what as they began to organize. "We really go by what we are good at" (Student C). Tasks individuals were responsible for related to different aspects of cyber defense. This expertise was sometimes described as familiarity with specific technology, such as HoneyBot, SecurityOnion, Ubuntu, Kali Linux, or Apache. Other times the technical expertise was expressed in more general ways, such as good with active directories, servers, system configuration, vulnerability scanning, or research.

5. COLLECTIVE LEARNING: TRIAD ANALYSIS

Activity theory is descriptive in nature and provides a framework for looking at the structure and development of human activities and individual consciousness (Nardi, 1996). The individual-based activity system is described in the *subject*, *activity*, *object* triad was originally put forth by Vygotsky in the late 1920s (Bakhurst, 2009). A beginner engages in activity (uses tools) to attain the object. Individual actions that make up the activity include not only internalizing knowledge but also express the ethics and dependability of behavior during system configuration. As the subject gains inside knowledge of system configuration, the quality of dependability assists the subject in being vigilant to offer dependable system configurations that are free from negligence and unintended consequences. The subject also applies ethics when making critical decisions. The theory of expansive learning states that learning is the result of the student working through transformations that result from engagement with the activity system. As the student cycles through performing actions that move toward achieving the object, the activity becomes internalized and goes from being an abstract idea to a more concrete understanding.

As Vygotsky illuminates the idea that learning is a socially mediated act (Cole et. al., 1978), the subject begins to interact and engage with the community to reach the object and learning outcome. The community governs professional norms, powers

the tools, and gauges collective goals through an organic division of labor. As a result, the subject takes actions to mature in problem-solving and technical trouble-shooting ability, reaching the consciousness of cyber defense as an intended outcome. The collective activity system is multilayered, multi-relational, and involves all four triads and all relationships between components. Toward this end, each of the triads within the activity system describes various types of mediation that affect the internalization of the activity within the mediating influence of the other elements of the activity system (Kuutti, 1996). This is illustrated in the following mediated relationships (see Figure 2 above): (1) subject, activity, and object; (2) subject, community, and rules; (3) community, division of labor, and object; and (4) subject, community, and object.

5.1 Mediated Relationship in the *Subject-Activity-Object* Triad

The subject moves toward the attainment of the object, cyber defense, by engaging in activities that center on the development of technological knowledge and skills and the mindset that supports engagement in these activities. As students participate in the assignment, they are exposed to a variety of security systems and mechanisms. The mediating effect of the activity on achieving the object is expressed through the motivations of the subject (individual as well as team) to defend the system, and enacting the activity transforms their understanding of cyber defense. This transformation was perhaps most evident in a rising consciousness of the enormity of the goal, transferring codified systems knowledge to implicit knowledge applicable in their situations and contexts, and the potential benefit of learning to think like a bad actor when taking a defensive position. Knowledge of the activity (tools) is pivotal to arbitrating the subject's ability to problem-solve to reach the object. Engaging in the activity transforms the subject, which in turn affects the activity. Achieving the object becomes streamlined as the activities become internalized and the conditions that call for specific activities become more reflexive.

5.2 Mediated Relationship in the *Subject-Community-Rules* Triad

The triad that describes the relationship between the subject, the community, and the rules can be seen as expressing the social context of the activity. Rules substantiate what it means to be a member of the community that shares the object (Kuutti, 1996). Rules and ethical codes of conduct mediate between the subject and the community. For these students, the most immediate cyber defense community they belonged to was the class context including the instructor and classmates which existed within a larger program of study within the school, within its college, and within the larger university. Certain rules were set down by the instructor in the assignment and others developed within the dynamics of individual teams. Both the instructor and classmates provide input as to what rules are expected in their professional field. While any set of rules can constrain or enable activities, knowing the rules is important to being part of the larger community where rules are established and debated. In addition to the instructor and classmates acting as a community, students (subject) engaged in internship experiences, Cybersecurity Club events, and open source community resources. These social engagements enhanced the subject's growing knowledge of these rules in articulating the ethics of their profession, their awareness of policy and procedures, and interest in conforming to professional norms.

5.3 Mediated Relationship in the *Community-Division of Labor-Object* Triad

Like activity, the division of labor is critical to the community's attainment of the object. In the context of the university, there are internal stakeholders who bear responsibility for the governance, administration, teaching, etc. that support students' efforts in the teaching and learning partnership. These students also benefit from stakeholders who are outside the university, such as professionals in the field and the open-source community. All of these stakeholders provide different kinds of labor and resources that support the goal of cyber defense. For the students in this class, the division of labor within teams is also important to the overall goal. The division of labor at the team level requires decisions about how to communicate and effectively operate to respond to the assignment. Among those interviewed, collaboration and division of responsibilities tended to be the norm; however, leadership within teams was not formalized. In one case, an individual claimed leadership of the team, but for the most part leadership in the teams was expressed through technical expertise and a desire to organize team activities. Overall, decision-making within teams respected the opinions of team members.

5.4 Mediated Relationship in the *Subject-Community-Object* Triad

Cyber defense as a goal supersedes the interests of any one individual. For this reason, the subject needs to be situated within a community that shares the goal. Both system defense and the development of a consciousness of cybersecurity require a socially mediated transformation. The community plays a part in this transformation by investing in supporting student attainment of needed skills and knowledge; assimilation of policy, procedure, and professional ethics; and through division of labor. Students enlarged their membership within the larger cyber defense community in part through the Cybersecurity Club, which many attended. The Cybersecurity Club not only helped the subject (students) learn new skills and knowledge while giving them the opportunity to interact with professionals in the field, but also infused the norms of professional practice and provided alignment between the subject's personal goals and the collective object of the community. Students displayed increased awareness of the importance of building relationships with the community for their professional growth and to adopt professional norms.

6. CONCLUSION AND CONTRIBUTION

This paper has demonstrated an educational intervention through the lens of activity theory designed to stimulate and increase cyber defense consciousness. This study describes student perceptions of a formative intervention deployed in a cybersecurity course. The qualitative analysis has revealed much about how these students at an early stage in the course are developing a consciousness of cybersecurity that involves the internalization of skills and knowledge; reliance on community for support, information, and acculturation; working with others through the division of labor; and their

struggle with the demands of cybersecurity work. By providing foundational knowledge and an array of tools, while requiring teams to take responsibility for their own systems and problem solving, students, working in a sandbox environment, were provided an experience that mimicked threats that are encountered by professionals responsible for system security and allowed for hands-on encounters with system challenges addressed through teamwork. This replicated many aspects of professional work in cybersecurity, including the need to manage personal learning, build relationships, and embrace the ethics and responsibilities of the position. Another important takeaway was the clear importance of community in and beyond the classroom both to the educational process as well as to continued professional development.

The study is unique in adopting activity theory in the context of understanding student perceptions of cyber defense work and also contributes in a practical way to information systems education by describing the factors that affect the development of technical and soft skills in a sandbox environment. The paper describes the theoretical development of cyber defense consciousness through the discussion of node analysis, with six components that include subject, activity/tools, object, rules, community, and division of labor. The paper further describes four mediating relationships among these six components. Cyber defense is a collective goal that is larger than any individual goal. As Crumpler and Lewis note (2019, p. 5) "The ability to work as a team is essential since cybersecurity is rarely handled by single individuals." This study illustrates and contributes to a pedagogical approach that transforms the cyber defense consciousness of students through the collective learning activity model. The limitations of this analysis are consistent with other qualitative methods. The findings cannot be generalized, but they can inform cybersecurity education and educational research in this area.

There is much left in this research stream to investigate. For example, students were exposed to a wide variety of tools but were not asked to evaluate the tools they were learning. The number and type of tools used were wide-ranging, designed to address different issues for various O/S, systems, applications, and networks. Each tool presents its own strengths and weaknesses to address specific technical problems. We focused on adopting/using/learning those tools that address various network and system security threats and analysis. Research that investigates student evaluation of tools may further inform how subject motivations in the use of specific tools affect both motivation and the objective. Future work is needed to explore the extent to which specific tools or activities can be mapped to specific outcomes as well as assess activities further to determine which are most efficacious in increasing student awareness and learning. These endeavors will be complicated by the fact that within the activity system the nodes do not stand alone. The learning outcome is embedded in the entire activity system, and the four mediated relationships all work to facilitate students' learning outcomes. Extensions of this work include replication of the intervention with other classes and an analysis of data collected at the end of the semester after students have taken on the role of a penetration tester to determine shifts in the object, transformations of the subject, changes in activities undertaken, and consciousness of cyber defense.

7. ACKNOWLEDGMENTS

The authors wish to thank Alison von Eberstein for her contributions to the interview questionnaire, consent form, and the Institutional Review Board (IRB) protocol approved by the Florida State University Human Subjects Committee. The authors also wish to thank Christy Chatmon for her efforts in interviewing participants and Vanessa Myron for transcribing interviews.

8. REFERENCES

Allen, D., Karanasios, S., & Slavova, M. (2011). Working with Activity Theory: Context, Technology, and Information Behavior. *Journal of the American Society for Information Science and Technology*, 62(4): 776-788.

Bakhurst, D. (2009). Reflections on Activity Theory. *Educational Review,* 61(2), 197-210.

BBC News. (2020). Coronavirus: US Accuses China of Hacking Coronavirus Research. Retrieved September 3, 2020, from https://www.bbc.com/news/world-us-canada-52656656.

Bellamy, R. K. E. (1996). Designing Educational Technology. In B. Nardi (ed.), *Context and Consciousness: Activity Theory and Human-Computer Interaction* (pp. 123-146). Cambridge, Massachusetts: MIT Press.

Bodea, C-N., Dascalu, M-J., & Cazacu, M. (2019). Increasing the Effectiveness of Cybersecurity Teaching and Learning by Applying Activity Theory and Narrative Research. *Issues in Information Systems,* 20(3), 186-193.

Cole, M. & Engeström, Y. (1993/2001). A Cultural-Historical Approach to Distributed Cognition. In G. Salomon (ed.), *Distributed Cognition* (pp. 1-47). Cambridge, Massachusetts: Cambridge University Press.

Cole, M., John-Steiner, V., Scriber, S., & Souberman, E. (1978*). L S. Vygotsky. Mind in Society: The Development of Higher Psychological Processes.* Cambridge, Massachusetts: Harvard University Press.

Crumpler, W. & Lewis, J. A. (2019). The Cybersecurity Workforce Gap. Center for Strategic & International Studies. Retrieved September 3, 2020, from https://www.csis.org/analysis/cybersecurity-workforce-gap.

Dawson, J. & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology,* 9, article 744.

Engeström, Y. (2019). *Learning by Expanding: An Activity-Theoretical Approach to Developmental Research (2nd ed.)*. Cambridge, Massachusetts: Cambridge University Press.

Engeström, Y., Miettinen, R., & Punamäki, R-L. (Eds.). (1999). *Perspectives on Activity Theory*. Cambridge, Massachusetts: Cambridge University Press.

Fulton, E., Lawrence, C., & Clouse, S. (2013). White Hats Chasing Black Hats: Careers in IT and the Skills Required to Get There. *Journal of Information Systems Education,* 24(1), 75-80.

Iyamu, T. & Shaanika, I. (2019). The Use of Activity Theory to Guide Information Systems Research. *Education and Information Technologies,* 24, 165-180.

Kaptelinin, V. (1996). Computer-Mediated Activity: Functional Organs in Social and Developmental Contexts. In B. Nardi (ed.), *Context and Consciousness: Activity Theory and Human-Computer Interaction* (pp. 45-68). Cambridge, Massachusetts: MIT Press.

Kuutti, K. (1996). Activity Theory as a Potential Framework for Human-Computer Interaction Research. In B. Nardi (ed.), *Context and Consciousness: Activity Theory and Human-Computer Interaction* (pp. 17-44). Cambridge, Massachusetts: MIT Press.

Nardi, B. (Ed.) (1996). *Context and Consciousness: Activity Theory and Human-Computer Interaction*. Cambridge, Massachusetts: MIT Press.

Schneider, F. B. (2013). Cybersecurity Education in Universities. *IEEE Security & Privacy,* 11(4), 3-4.

Spasser, M. A. (1999). Informing Information Science: The Case for Activity Theory. *Journal of the American Society for Information Science,* 50(12), 1136-1138.

Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., & Askwith, B. (2016). Cyber Security Teaching and Learning Laboratories: A survey. *Information & Security: An International Journal,* 35, 51-80.

Topi, H. (2019). Refelctions on the Current State and Future of Information Systems Education. *Journal of Information Systems Education,* 30(1), 1-9.

Verizon. (2019a). *2019 Data Breach Investigations Report (DBIR)*. Retrieved September 3, 2020, from https://enterprise.verizon.com/resources/reports/dbir/.

Verizon. (2019b). *2019 Data Breach Investigations Report (DBIR). Executive Summary*. Retrieved September 3, 2020, from https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf.

The Wall Street Journal. (2020). U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research. Retrieved September 3, 2020, from https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205.

AUTHOR BIOGRAPHIES

Melissa Gross is a professor in the School of Information at

Florida State University and a past president of the Association for Library and Information Science Education (ALISE). She teaches and does research in the areas of information seeking behavior, research methods, program and service evaluation, and information literacy. She has published extensively in a variety of peer-reviewed journals, including *Library and Information Science Research*, *Library Quarterly*, *Journal of the Association for Information Science & Technology, and College & Research Libraries*. She has authored, co-authored, or co-edited 12 books. Her forthcoming edited book, with co-editor Julia Skinner, is *Working with Underserved Students on Campus and Beyond: Meeting the Information Needs of People Facing Trauma, Abuse, and Discrimination* (Libraries Unlimited).

Shuyuan Mary Ho is an associate professor in the School of

Information at Florida State University. Her research focuses on trusted human-computer interaction, including computer-mediated deception, cyberbullying, cloud forensics, cyber defense education, and socio-technical behavioral experiments. Her work appears in over 60 journal articles and conference proceedings, including *Journal of Management Information Systems*, *Computers in Human Behavior*, *Computers & Security*, *Digital Investigation*, *Information Systems Frontiers*, and *Journal of the Association for Information Science and Technology*. Her work has been funded by the National Science Foundation and Florida Center for Cybersecurity, and has been featured in the popular press, e.g., NPR, WIRED, and Forensic Magazine.

Appendix. Tools Identified by Students

Offense/Attack Tools: Examples	Defense Tools: Examples
Malware	
Backdoor malware: Malware, ransomware, Trojan horse, thumb print	**Antivirus**: Windows Defender, Malware Bytes, Webroot, Avira, Avast, Microsoft Security Essentials, Antivirus popup blocker, Norton Antivirus, Mcafee Antivirus, Kaspersky, Clamscan
Ransomware: Ransomware	
Password	
Password cracker: Password cracker, John the Ripper	**Encryption**: BitLocker on Windows, encryption
Brute force: Password cracking, dictionary attack, Python script	**Access control**: Passwords, Bell-LaPadula model, Biba model, RBAC access control model, read/write permissions, least privilege access
	Authentication: User account, key pass, active directory
	Remote administration; Using remote administration, remote scan and administer
Database	
SQL Injection: Injection attacks	**Database knowledge**: MysQL, Transact-SQL (or, T-SQL) for Sybase and Microsoft, RAMQ database, database
Systems and Servers	
Scripting: SQL injection, cross-site script attacks, script attacks, basic command line attacks	**Scripting**: php; Vi, Emans and Atom text editor for Linux/Unix-based scripts, Python script, script attacks against Java or Adobe, scripting
	Extensions: Install browser extensions to block popups
	Browser knowledge: Safe browsing, don't click on ads while browsing, do not go to crazy sites or download stuff during online shopping.
	Website knowledge: Permission on files, deploying web application, tunnel/backdoor on website, configuring a LAMP server (Linux, Apache, MySQL, php), Nessus vulnerability scan on website, "know not to go to websites that look fishy"
	OS knowledge: Windows, Linux O/S, Ubuntu, Ubuntu Mac, Web cast flows, LAMP server, Debian Linus O/S, Ultimate Boot CD, Deep Freeze on Windows, Apache server, operating systems
	Software updates and patches: Apache, Nessus Lamp server, Php, software update, patches, patching webserver
	Systems and servers: Basic command line, Windows server, Kali Linux, honeypot server, ping the system, Ipconfig the system to find IP addresses, Linux commands, Oracle server, Ubuntu Linux, enabling serve BITS (background intelligent transfer service), SQL server, Web server, Debian Linux, Palo Alto Networks, Cisco Firewalls, Security Onion system, MBT server configuration, DNS server for name resolution, DHCP server assigning IP addresses
Phishing emails/calls: Reconfiguring email servers to flag emails outside the network: Spear fishing attacks, social engineering, phishing	**Honeypots**: HoneyBot, kfSensor honeypot, honeypot
Network Penetration & Defense	
DDOS: DDOS, SYN Flood, DDOS on TCP, UDP open ports	**Firewalls**: Firewalls, intrusion detection systems, intrusion prevention systems, pfSense, Juniper, Comodo, Iptables on Linux, Cisco adaptive security appliance 5500-X series, Palo Alto Networks, Windows Defender, Cisco Firewalls
Scan: Nikto, Wireshark, Zenmap, remote scan, port scan	**Scan or filtering**: Zen map, Nessus, Nikto command-line vulnerability scanner, Microsoft Safety Scanner, nmap, Webroot, Metasploit, Rootkit Hunter, Kali Linux, EtherCap

	port scan and packet analysis, malware scanner, vulnerability scanner, scan IP addresses,
IP spoof: Wireshark	**Network knowledge**: Wireshark, network mapping, packet monitoring Cisco, Palo Alto Networks, Kali Linux, Metasploit, network topology, http vs. https traffic, Ether Ape ECP and UDP ports, IDS, SIEM, routing, switching, reconfigure networks
Kali Linux: Kali Linux, Armitage, Metasploit	**Penetration testing**: Kali Linux, Wireshark, Metasploit, brute-force attack, Armitage, EtherCap, Burp Suite, Nessus
Exploitation: Offensive port scan on Kali Linux, Rootkit, Wireshark, Armitage. Ubuntu exploits, memory-based exploitation, open TCP/UDP ports	**Intrusion detection**: Security Onion, Wireshark, Alien Vault, Splunk, intrusion detection system, security information event management, checking traffic logs, discovering "a tunnel or backdoor where you can send files in and out"
DNS attack: DNS vulnerabilities	**Data analytics tools**: Alien Vault, Splunk
Law & Policy	
	Law and policy: Cat Card, disaster recovery policy, account policy, email policy, security policy, firewall rules, password policy, privacy law, military policies,
Physical Security	
	Forensics: Computer forensic
	Backup or recovery: Deep Freeze; backup files, data, server; recover information from backup
	Offline: Shut down or isolate system from network, take computer offline to avoid attacker
Virtualization	
	Virtualization: Virtual machines, sandbox virtual environment, Microsoft Hyper-V Management, Oracle VirtualBox, Kali in VirtualBox,
	Reimage computer: Reimage the virtual machines, reimage computer
Personnel Security & Training	
	Security clearance: Security clearance, CatCard
	Training: Awareness of spear phishing attacks, formal training, hands-on training, educating the end user, compliance training, security ops
	Online reference: Google, Google exploits, Stack Overflow, Github, Web browser, Whois

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872