Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness

*Shuyuan Mary Ho**, *Melissa Gross*

School of Information, Florida State University, Tallahassee, FL 32306-2100 USA

ARTICLE INFO

Article history:
Received 18 November 2020
Revised 6 May 2021
Accepted 30 May 2021
Available online 20 June 2021

Keywords:
Human-computer interaction
Activity theory
Organizational learning
Computer incident response
Cybersecurity operations

ABSTRACT

Cloud environments enable organizations to offer uninterrupted delivery of information and services to their subscribers. Unfortunately, these platforms also create opportunities for cyber-attacks. As organizations become increasingly virtual, the channel that enables authorized users to access targeted information becomes the same channel used by hackers to propagate mischief. Cyber defense has thus become a dynamic challenge in the ever-connected cloud space. This study adopts the lens of activity theory to conceptualize cyber defense as an activity system and offers a transformative approach to developing organizational cyber awareness. The study contributes to organizational collective learning mechanisms in building effective computer incident response teams for cybersecurity operations.

1. Introduction

The interaction between cyber-defense and cyber-attack resembles a rigorous game of chess. Cybersecurity professionals are commissioned to protect information assets and cyberinfrastructure, while attackers—such as lone-wolf hackers or state-affiliated organized criminals—seek every opportunity to gain access and bypass security countermeasures that protect systems and networks. The hacking of U.S. federal government agencies' email systems, as an example, represents many serious and ongoing infractions (Cohen et al., 2020; BBC 2020; Sanger, 2020; Diaz, 2020; Bing, 2020). Whenever an access control mechanism presents a barrier, hackers will attempt every possible strategy to escalate their privileges to gain access. Moreover, remote administration access can be exploited by hackers to gain stealthy access to systems and networks, and encryption mechanisms can be weaponized to hold information for ransom. Organizations can suffer the threat of data loss for a variety of reasons.

To effectively counter rigorous cyber-attacks, organizations are urged to enhance their cyber defense and further develop organizational cyber awareness, which is a consciousness within the organizational culture of the need to protect information assets. Organizational cyber awareness requires more than knowledge transfer and retention. It requires the development of a cyber-defense consciousness so that organizations can properly position themselves to be ever vigilant in the dynamic cyber chess game. Thus, organizations require cyber professionals that are not only technically savvy with up-to-date cyber defense knowledge but also equipped with a keen awareness of creative breaches and system breaking/cracking techniques, along with troubleshooting abilities that prepare them for future cyber-attacks. This interactive chess game between hackers and cyber defenders represents a grand challenge to organizational cybersecurity objectives.

* Corresponding author.
E-mail addresses: smho@fsu.edu (S.M. Ho), mgross@fsu.edu (M. Gross).
https://doi.org/10.1016/j.cose.2021.102357

As cyber-attacks increase and become more complicated, developing a consciousness of cyber defense ought to be the primary objective in organizational governance of information systems.

Organizations can be considered sociotechnical systems with intertwined social and technical factors that impact their governance and operations (Bostrom and Heinen, 1977; Bostrom and Heinen, 1977; Sawyer and Jarrahi, 2014). To address the grand challenge of defending organizations against an everchanging cyber chess game, our research question is quite focused: *how do we develop and enhance cyber defense consciousness within organizations?* We conducted a study where cyber defense is conceptualized as an activity system, and the activity itself provides useful context Nardi (1996). A collective activity system was created in a cloud-based laboratory sandbox using virtual machines and networking connectivity. The next-gen cybersecurity professionals, students in an advanced cybersecurity class, were tasked as cyber defense teams to set up their systems, networks, and information assets. Each team was then charged to protect their organizational information assets, while also identifying the vulnerabilities of the other groups' systems and networks. Through the interactive cyber defense and offense activities, each group of participants learned to handle and respond to computer incidents. Participants were interviewed, and the interview transcripts were analyzed to identify not only individual learning systems, but also collective learning systems for organizational cyber defense operations.

2. Background

Information and communication technology (ICT) enables organizations to become virtual. Handy (1995) challenged managers, organizations, and society to consider the implications and dilemmas of virtuality. Virtuality has not only redesigned organizational norms and workflow—where information and people meet in cyberspace—but has also redesigned our cities where skyscrapers are no longer the center of attention, as organizations no longer require a physical address with dedicated locations. Business meetings can take place from home, in a coffee shop—anytime and anywhere you have a communication device that connects to the cyberinfrastructure. Mowshowitz (1997) illustrated several instances of virtual organizations. As organizations store information in the cloud—whether public, private, or hybrid—the virtual storage of information enables *virtual memory*. Virtual machines (e.g., VMware, Oracle VirtualBox, Azure) make network switching a virtual activity facilitated by *virtual switches*. In the same way, team members can be grouped into *virtual teams* to work on task assignments with shared goals and shared identity. Our existence and experience of the physical world becomes a *virtual reality*. The instances of virtual constructs can go on and on to include *virtual office, virtual classroom*, and *virtual community* (Mowshowitz, 2000). However, organizations still operate based on basic trust (Handy, 1995).

Knowledge workers can get psychologically attached to their organization, and this organizational identification will help determine their beliefs and behavior (Dutton and Dukerich, 1991; Dutton et al., 1994). Wiesenfeld et al., 2006; Wiesenfeld et al. (1999) suggested that just as organizational identification provides the social and psychological tie that brings workers and the organization together, workers' *virtual status* can moderate the relationships between communication media and the organization. More specifically, the use of electronic communication defines the high virtual status through which workers create and sustain their organizational identification. As knowledge workers interact virtually, Larsen and McInerney (2002) urged that knowledge workers be equipped with ethics, problem-solving ability, and associated skillsets—and that organizations allow trust to mediate virtual workers' effectiveness and efficiency.

2.1. Organizations as sociotechnical systems

The term sociotechnical systems (STS) was first articulated by Trist and Bamforth (1951) in their case study of a coal-mining business that was losing productivity despite mechanization. Their evaluative approach took both interactive technological and sociological patterns into account in assessing the resulting psychological effects experienced by workers. Bostrom and Heinen (1977) stressed that the MIS development problems in organizations involve mostly behavioral problems. When user behavior is not considered in MIS design and development the result is inadequate system design. Thus, sociotechnical systems (STS) are characterized as both social and technical systems that are "jointly independent, but correlative interacting systems," to address the design issue [(Bostrom and Heinen, 1977), p. 17]. Emphasis on either a machine theory or a human-centric theory is inadequate and will result in system design failure. Bostrom and Heinen (1977) suggested a collaborative design approach is required to understand who is in charge, and incorporated dynamic factors in the design to overcome a static view of systems. [Liu et al. (2006), p. 521] raised two important claims of STS theory. First is the focus on the "joint optimization of the technical and social aspects of an organization," and second is that the design should "meet the demands of the external environment."

Sawyer and Jarrahi (2014), on the other hand, identify three important elements that serve as a basis for sociotechnical system development. The first element is a mutual constitution; it is important to consider a phenomenon without making a prior judgment regarding the significance of its social or technological aspects. Both humans and technologies may have some agency, and their actions are not deterministic. Second is the recognition that all technologies are embedded in a social context, and both adapt to and help reshape the social world. The third is collective action. It is important to understand the joint interests and multiple goals that are intertwined with both the social context and the technological elements, recognizing the complexity and uncertainty involved in the process of change both technically as well as socially within the organization.

2.2. Computer Incident Response and Cyber Defense

Organizations function normally when a business operates as expected. However, when crises or unexpected situations happen—such as distributed cyberattacks (Kurt et al., 2018),

organized crime (Chambliss, 1988), advanced persistent threat (APT) (Ahmad et al., 2019), or pandemic crisis Peckham (2013), organizations' losses can be drastically multiplied. Organizational incidents can be defined as the interactive complexity and sociotechnical problems occurring between the unfamiliar/unsafe conditions and ignorant/risky behavior of workers within organizations. Computer incidents specifically refer to computer-related accidents that can potentially jeopardize the confidentiality, integrity, and availability (CIA) of information systems—and information being stored, transmitted, or processed in violation of standard corporate information policies. Incident response evolves from rudimentary problems (e.g., internetworking, printer/projector issues) to encompass computer incidents (e.g., malware, worms, viruses and APT). Cooke and Rohleder (2006) modeled an incident learning system based on the theory of incident learning to reduce unsafe conditions and the severity of incidents. This model and the incident reporting system afforded organizations a mechanism to learn, to respond to, and to handle crises, incidents, and emergencies vigilantly.

Chen et al. (2007) adopted coordination perspectives to study the nation's critical incident response systems. Particularly, the dependencies between actor-activity, activity-activity, and actor-actor were studied to derive design principles for a fire department's emergency response systems across multi-incidents of a chemical fire. This study identified coordination interdependencies and interaction effects in emergency response management systems. Mitropoulos et al. (2007) proposed a role-based access control approach to investigating these incidents across distributed information systems. Drtil (2013) analyzed the impacts of computer incidents from the CIA triad standpoint and suggested multiple sociotechnical precautions for management to consider. Ruefle et al. (2014) documented the practitioners' perspectives of an incident handling lifecycle and the activities involved in this process. Although organizations generally have some plans and procedures in place for incident management, Hove et al. (2014) identified incident response challenges—as well as the lack of synchronicity in incident information collection, communication, dissemination, and reporting throughout organizations. Organizations tend to determine predefined controls to prevent dynamic threats. However, this control-centered management approach may not work effectively in unexpected or exceptional threat situations. By contrast, Baskerville et al. (2014) proposed a forward-thinking incident-centered framework to pivot between prevention paradigms and response paradigms.

Computer incident learning and response continue to evolve into a collective response mechanism—the organizational computer security incident response team (CSIRT)—that begins with the Computer Emergency Response Team Coordination Center (CERT-CC) at Carnegie Mellon University (CMU) in 1988. Ahmad et al. (2012) conducted a case study based on a financial firm with a global presence, identifying the challenges in building and supporting CSIRT. Grispos et al. (2015) proposed a set of security incident response criteria (SIRC) that expands the horizon of incident handling lifecycle to further include multidisciplinary CSIRT with dynamic stakeholder involvement and access to and protection of digital evidence/data from a practitioner's perspective. Ahmad et al. (2015) further identified organizational learning perspectives in incident response and handling and noted challenges in security intuiting, attending, interpretation, experimentation, integration, and institutionalization, as well as mechanisms of feed-forward and feedback. As novel as the incident-centered framework is (Baskerville et al., 2014), an organization's readiness to address dynamic cyberattacks must be measured by its sound security operations. Ahmad et al. (2020) proposed a joint framework integrating information security management (ISM) and incident response (IR) functions, to secure an organization's digital assets. Moreover, Ahmad et al. (2021) proposed a process model that explains the role of management practice in developing and improving an organization's situational awareness during incident response.

Brown et al. (2016) acknowledged the internalization/ externalization influences between individuals and the social contexts as posited by activity theory and conducted an ethnographic study of CSIRT's in security operations centers (SOCs). The study identified gaps between standards and incident response work, team formation, and the internal and external relationships with multiple stakeholders (e.g., team coordinators, customers, and vendors). Acquisition of tools for communication among teammates, tools for collaboration with vendors, and tools for both technical and nontechnical problem-solving have become a predominant success factor. Bartnes et al. (2016) studied the incident response challenges of electrical power companies and suggested the urgency of establishing cross-functional teams to address the organization's ability to learn and respond to future incidents. McLaughlin et al. (2017) surveyed industry and suggested that in addition to competent technical skills and expertise, incident responders require the cognitive ability to distill information, along with attention to detail, communication skills, management knowledge and influence, leadership quality, and passion for information security. Nyre-Yu et al. (2019) adopted ethnographic methods to study active CSIRTs. Their findings suggested distributed expertise, shared awareness and knowledge sharing across secure, mission-critical task contexts.

2.3. *Organizational readiness for cyber defense*

Organizations should not only implement preventative, protective, and detective controls but should also be ready to deploy "offensive defense." Fulton et al. (2013) emphasized the important role of 'white hat' professionals. Organizations should prepare themselves using penetration testing to identify vulnerabilities within existing systems and networks. Schneider (2013) pointed out weaknesses in the current cybersecurity workforce and the lack of adversarial thinking in organizational cyber defense methodologies. Topham et al. (2016) discussed the importance of and requirements for cybersecurity laboratories (e.g., physical laboratories, simulations laboratories, virtual laboratories, and hybrid laboratories). Cybersecurity laboratories can enhance organizational awareness and learning with positive impacts on cyber defense. Dawson and Thomson Dawson and Thomson (2018) suggested both systemic thinking and team player mentality as key traits in building the cybersecurity work-

force within an organization. Technical and social skills are equally important Crumpler and Lewis (2019). The ideal cyber defender should have emotional intelligence while being able to communicate technical solutions to both management and the public. Employee loyalty, ethical commitment, and civic duty are required of the cybersecurity professional. Ho (2020) also emphasized trustworthiness as the top quality for cyber information professionals.

In sum, an organization's readiness, conscious awareness, and the ability to respond to and handle computer incidents still require much work. As computer incident response and cyber defense operations become critical to maintaining an organization's normal operations, our study has been framed to first understand activity theory, and then consider cyber defense as an activity system.

3. Activity theory

Activity theory originated in the work of Vygotsky in the early part of the 20th century Vygotsky (1978) and has demonstrated value in information science where it has been used to design, develop, and understand information systems, particularly in terms of the social context of systems (Allen et al., 2011; Iyamu and Shaanika, 2019; Nardi and Nardi, 1996; Spasser, 2000; Chen et al., 2013). Many theorists have added to the activity theory model [e.g., (Leont'ev, 1929; Leont'ev, 1974; Leont'ev, 1978; Leont'ev, 1978)], but Engeström has done much to produce the integrated model that is commonly in use (Engeström, 1987; Engeström, 1990; Engeström, 1990; Engeström, 1999; Engeström, 2000; Engeström, 2001; Engeström and Sannino, 2011). Engeström (Engeström, 1987; Engeström, 1990) defined the term 'expansive learning' as being a collective activity where multiple individuals are involved in taking actions to transform an activity system. During the transformation process, the actors collectively reconceptualize the associated objects and motives of the activity to embrace a wider horizon of possibilities. Two types of activities were discussed in the human activity systems proposed by Engeström (2001). The basic activity model is *individual*-based, where a subject uses a tool to achieve an objective (object). However, he extends this individual model to incorporate social actions taken *collectively* within a group (community) (Iyamu and Shaanika, 2019; Engeström, 1990; Engeström, 1990).

Leont'ev (1974) offered a fundamental perspective on the "influence" of the subject, and a response phenomenon (both subjective and objective) regarding that influence. The discovery of this feedback loop on behavior enlightened [Leont'ev (1974), p. 7] to propose the concept of information flow, which transforms the subject inwardly through external activities, and this transformation of the subject also involves "culturology;" the cultural factors that influence the subject. In this dyad, the subject and object are in a reciprocal relationship. The subject transforms the object, and the properties of the objects also transform the subject. The internalization reflects the external activity. Activity describes the mechanisms of mental processes—from internalization to externalization. This mental process acquires a structure that is linked to the means and modes—socially and historically formed—transmitted to the subject (Leont'ev, 1974). Activity, thus, is the human mind existing and expressed as 'consciousness' that emerges in the interaction with the objective reality as activity (Kaptelinin, 1996; Kaptelinin, 2005).

Under the broad umbrella of information science, activity theory has been applied in computer-supported collaborative work (CSCW) (Kuutti and Arvonen, 1992), HCI (Nardi and Nardi, 1996; Engeström, 2008), information systems (Iyamu and Shaanika, 2019; Kuutti, 1999; Karanasios and Allen, 2018), information behavior (Allen et al., 2011), and computer-supported collaborative learning (CSCL) (Prapinpongsadorn et al., 2017) to further understand the sociotechnical aspects of the design and development of systems as well as to describe the context within which system work is undertaken.

Activity requires that the objective features of a system be meaningful to humans. This includes culturally and socially determined objects such as shared identity, values, and beliefs. These objects determine the way people act and react in any environment. To be precise, activities are considered to be more than a process; *activities* involve the motives of the subject. Each motive establishes an object whether material or conceptual, whereas *processes* are about the actions taken to achieve a specific goal (Kaptelinin, 1996). Activities are mediated by various artifacts such as instruments and signs. The subject-object interaction is not only mediated by *tools* but also mediated through *community*. In the activity systems, there are three mediational means: (1) *tools* are for subject-object interaction, (2) *rules* are for subject-community interaction, and (3) *division of labor* is for community-object interaction Kaptelinin (1996). Extended from the concept of "culturology" (Leont'ev, 1974), [Kuutti (1991), p. 533] further suggested "cultural mediation" as a factor embedded in situations; that is, the "cultural heritage of the situation." Many of the concepts and relationships in activity systems are developed historically and situated in the course of the cultural process.

One important theoretical stance is that activities provide context. As the basic unit of analysis, activity provides a meaningful context for individual actions Kuutti (1991). As active actors who understand the motive of the activity, subjects can be either *individuals* or a *collective* Kuutti and Arvonen (1992). When compared with frameworks of situated action Suchman (1987) and distributed cognition Cole and Engeström (2001), activity theory provides a cultural-historical approach to observe and understand users' objects and motives, and discover broad patterns of activity and the richness of context (Nardi, 1996). Cole and Engeström (Cole and Engeström, 2001) suggested using this cultural-historical approach to think about the distribution of cognition in subjects as well as in groups, across time, in the social world. The historical analysis of development can uncover the activity system, and we can learn about complex phenomenon by adopting this scientific approach Kaptelinin (2005).

Kuutti (1995) pointed out a crucial perspective that contradictions are often viewed as problems or breakdowns. However, contradictions are necessary for the development of an activity system. There will be no development in the associated activity systems until the contradictions and problems are overcome. Allen et al. (2011) suggested examining the tensions and contradictions in activity systems to pro-

vide insights for understanding organizational change. Contradictions can be considered a management tool for organizations intending to grow without radical transformation [(Engeström, 2008), p. 258]. Here, we could view computer incidents (i.e., sociotechnical problems) as a type of contradiction occurring within the organization (Ho et al., 2019). If an organization addresses 'problems' (i.e., computer incidents) appropriately and effectively, the organization will experience a chance to transition to a more secure organization. Computer incidents can be viewed as contradictions that create an opportunity for an organization to advance and be transformed into a more secure organization. Without the incidents, organizations would never realize their vulnerabilities. The occurrence of incidents can cause the organization to grow and transform.

There have not been many cybersecurity-related studies that adopt the lens of activity theory. Bodea et al. (2019) identified cybersecurity education challenges in IS disciplines. The foremost challenge is the balance between theoretical knowledge and practical experience in cybersecurity as both emphases are important. Collaboration with IT professional companies can help influence and infuse confidence in students when learning about modern enterprise-wide technical solutions. The inflexibility of organizational rules, as well as insufficient support from the university's administration, can prohibit learners from fully comprehending cyber threat simulations. Bodea et al. (2019) further substantiated with evidence that students learn better in small classroom settings; it is harder for instructors to sufficiently answer questions in a large class setting.

As activity theory has not been widely adopted to study cyber defense, we aimed to study cyber defense through the lens of activity theory and conceptualize cyber defense as an activity system. The cyber defense activity system in this study explores the perceptions and experiences of students in an advanced cybersecurity class who worked in teams to acquire and abide by the rules as regulated/projected within the community and to adopt/utilize multiple tools as artifacts to achieve the objective of protecting their information assets, systems, and networks as intended outcomes (Ho et al., 2019; Ho et al., 2019; Ho et al., 2017).

4. Method

Cyber defense is conceptualized as an activity system where the interaction between cyber defenders and attackers was simulated in a cloud-based laboratory space. Both social and technical components were designed in these simulations of cyber defense. Actors (i.e., defenders and attackers) met in the cyberspace where system administrators (as cyber defenders) configured and protected their organizational systems using state-of-the-art technologies, and the competing teams of hackers (as cyber attackers) used all available opportunities, tools, and techniques to penetrate the organizational space. Computer incidents occurred when defenders faced cyber-attacks from the opposing teams. Computer incidents are viewed as sociotechnical problems and contradictions that create an opportunity for the cyber defense teams to learn and to respond to attacks.

4.1. *Participants' characteristics and readiness*

Advanced IT students, who are next-gen cybersecurity professionals gave consent to participate in this study. These senior students had IT work or internship experience in either companies or the military, and had claimed majors in IT with a concentration in cybersecurity. These students met class pre-requisites of O/S systems knowledge (e.g., Linux and Microsoft), database management, web programming, networking and communication systems, and fundamentals of information security. They had appropriate technical skills, like systems configuration, deployment, and troubleshooting (for example, firewalls, intrusion detection, honeypots, and various virtual machines utilizing networking protocols as illustrated in Fig. 1). The tasks performed by the participants included setting up their organizational information assets (i.e., information systems and private networks), protecting their systems, identifying/correcting vulnerabilities, and engaging in incident response activities to prevent future attacks.

4.2. *Research design for cyber defense simulation*

Participants were first grouped into four virtual teams before setting up their information assets (Fig. 1)—in the form of virtual machines in a sandbox environment. Participants were charged to set up their organizational information assets, systems, and networks. The 'offensive defense' theoretical assumption was designed into these exercises to stimulate cyber defense awareness. That is, once their systems and networks were configured, participants were also charged to identify vulnerabilities and penetrate other teams' systems and networks. As a result, all teams faced cyber threats from other virtual teams that attempted to poke at their information assets. Each team's mission has thus become to protect their organizational information assets during computer incidents. When computer incidents occurred, these students were required to handle, report, and respond. These cyber defense exercises required that students not only troubleshoot computer incidents per se, but also to operate as a team—i.e., a CSIRT—to protect their organizational information assets. Participants were encouraged to be entrepreneurial, taking the initiative to troubleshoot their system and network environments, demonstrating both defensive and offensive defense skills.

4.3. *Laboratory design*

The laboratory exercises were designed and used to train cyber defenders annually from 2013 through 2020. Participants were organized into four teams of four to five members to gain hands-on experience with security tools designed to protect their workstations and web servers (either a Windows Apache 2.2 server or a WordPress on Lamp Ubuntu 12.02.1 server) in demilitarized zones. The security tools included defensive firewalls (e.g., Palo Alto Networks and pfSense) and intrusion detection monitors (e.g., Security Onion, Wireshark, and HoneyBOT), and penetration tools (e.g., Kali Linux). The Microsoft Hyper-V Management system provides the virtual lab platform that simulated a real-world cloud computing environment. Fig. 1 illustrates the expected network topology.

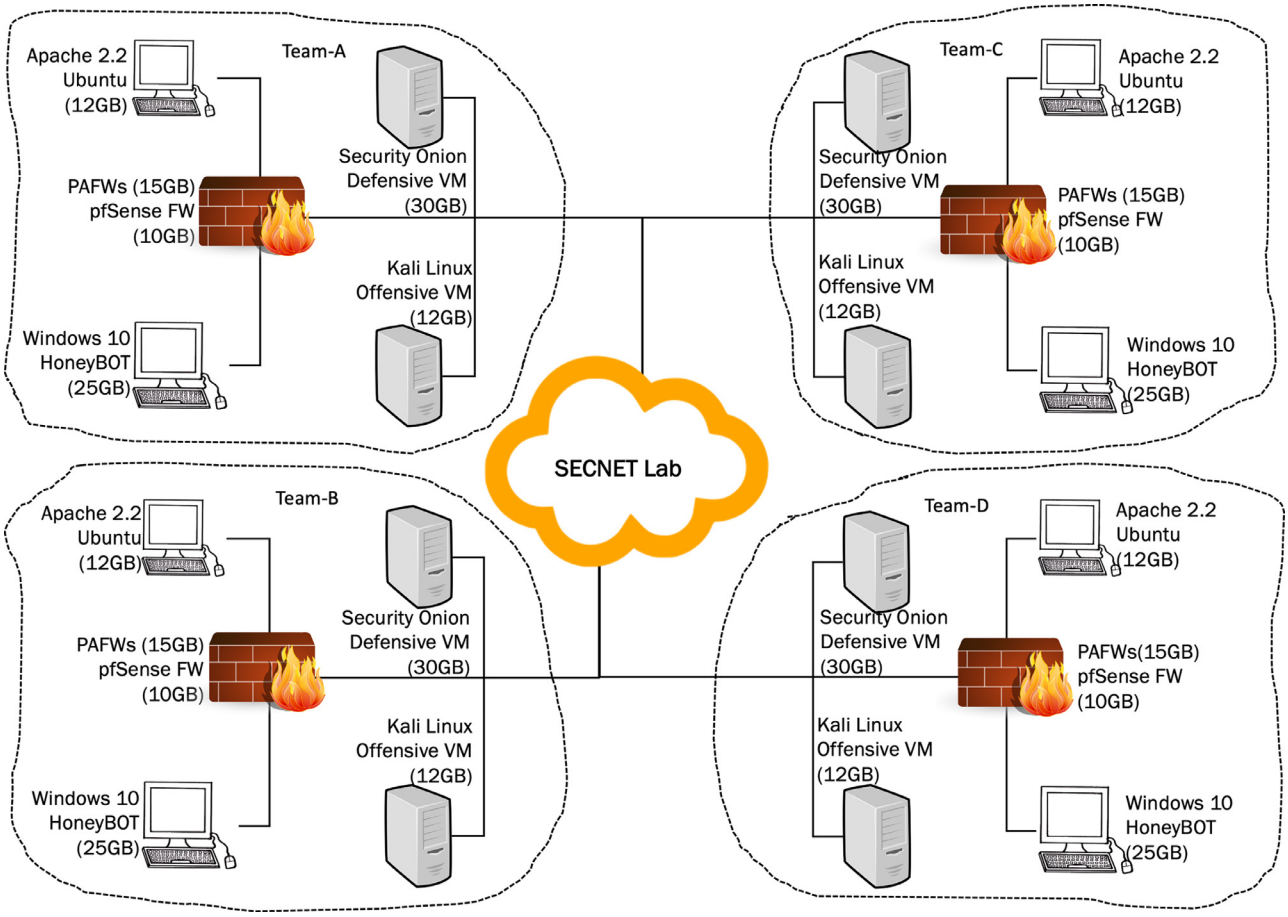

Fig. 1 – Cyber Lab (Gross and Ho, 2021).

4.4. *Data collection*

The cyber laboratory experiments were set up on a server powered by a Hyper-V management system, maintained by the Florida State University College of Communication and Information Technical Support Team. Data were collected from an advanced information security class offered at the Florida State University during Spring 2017. (The study was approved by the Florida State University Human Subject Committee and obtained the Institution Review Board protocols #2016.19676, #2017.22357, and #2018.25742.) We interviewed participants asking them to respond from the point of view of a "systems administrator" in the cyber defense team during the initial phase of the experiments.

Semi-structured, one-hour interviews were performed to capture the perceptions and experiences of advanced students operating as system administrators/cyber defenders. All interviews were digitally recorded and then transcribed for analysis. A total of 18 participants were recruited, and 15 agreed to participate in the interview; one was female, and the rest were males. One interview was not recorded, and one other resulted in an incomplete transcript due to the poor recording quality. As a result, 13 transcripts were analyzed. Interviews took place to investigate a hands-on laboratory project where they were learning both defensive and offensive skills. The interview questions were designed to probe the perceptions and experience of participants concerning the central concepts embedded in Engeström's activity theory model Engeström (1990). For example, participants were asked to describe their objectives, how they worked within their teams, relationships within the community, rules that govern cyber defense, division of labor, and so on.

5. Data analysis and findings

An initial coding scheme for the study was developed based on the elements of the activity systems framework and was deployed in NVivo12 during 2019. Transcripts of the interviews were also uploaded to NVivo12, and analyzed by two coders using the initial coding scheme. An iterative cycle of performing inter-coder reliability (Kappa) tests was instituted, comparing coding structures and revising and adding new codes based on the themes that surfaced from the data. Modifications of the coding scheme improved the Kappa scores from a range of 0.72 (fair to good) to 0.93 (excellent). Analysis of the coding revealed that differences in individual coding did not represent a lack of agreement, but rather were a result of the interdisciplinary differences between the coders which resulted in more extensive coding as codes were accepted based on discussions of the transcripts.

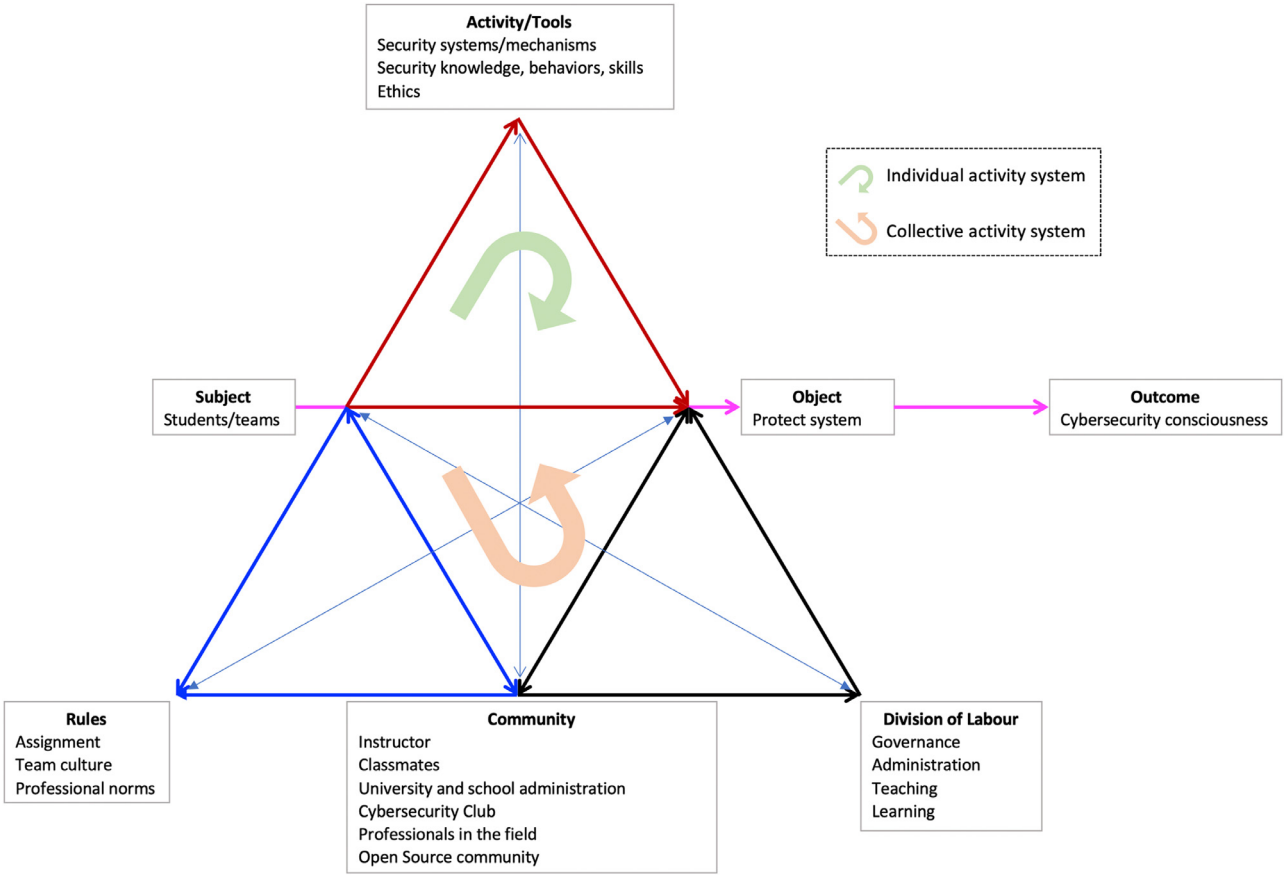

Fig. 2 – Cyber Defense Activity System (Engeström, 1990, Gross and Ho, 2021).

As individuals, teams, organizations, and communities are involved, culture and norms evolve. Although the objects and goals of protecting information and systems were clear and simple, a wide range of tools, activities, and technologies were adopted and deployed in the study. Thus, the coding scheme was revised to reflect the extensivity of the concepts. The coders met regularly to review each other's codes and agree on the addition of new codes as necessary. The resulting analysis informed the production of the cyber defense activity system (Fig. 2), which describes the development of cyber defense consciousness.

A beginner subject acquires tools to attain the object. Individual actions include not only knowledge of the systems, but also the ethics and dependability of behavior during configuration. As the subject gains inside knowledge of system configuration, the quality of dependability assists the subject in being vigilant to offer reliable system configurations that are free from negligence and unintended consequences. The subject also applies ethics when making critical decisions. We use the abbreviations (e.g., CD.03, CD.06, etc.) to reference the anonymized subjects. Findings are discussed below:

5.1. *Cyber defenders as individual subjects and cyber defense teams as collective subjects*

Participants initially felt confused, and somewhat intimidated by the field of cybersecurity. They felt they had insufficient technical knowledge and research experience to participate. For example, subject CD.04 found the activity of learning the penetration testing tool to be difficult, and subject CD.07 was confused about the functions of ZenMap vs. honeypot. Subject CD.12 wished that s/he started preparing for a cybersecurity career earlier to acquire industry-related certificates e.g., Cisco, Microsoft, ethical hacking, CISSP, etc. Subjects CD.03 and CD.07 showed low confidence in networking and firewall administration.

However, as the training proceeded, subjects CD.03, CD12, CD.13, and CD.14 began to become more active and knowledgeable. Curiosity was reportedly the primary driving force for learning about cybersecurity. Subjects CD.07 and CD.09 attempted to "figure stuff out," and subject CD.09 suggested research skills would be helpful, and subject CD.13 suggested, "you can do research yourself if you are interested." Hands-on learning provided subjects with an experiential learning opportunity, as demonstrated by subject CD.10 who worked alone to learn how Kali works. Knowing the importance of the technical "hard skills" subjects CD.05 and CD.06 also recognized the importance of soft skills (e.g., communicating in teams, asking the right questions, etc.). Technical problem-solving is the most basic and critical trait, along with being an approachable, communicative, and trusted teammate.

There were quite a few participants who changed their career path from programming and computer science to IT security as a result of their participation. These participants recog-

Table 1 – Cyber Defense Tools and Activities.

Defense tools	Specificities of knowledge
Anti-malware, anti-virus	Systems-based or browser-based anti-malware and popup blocker.
Password protection	Encryption, access control, authentication, remote administration
Database knowledge	Prevention of SQL injection (SQLi), inferential attacks, and attribution of data
Systems and Servers	O/S knowledge, coding integrity/quality, prevention of code injection and buffer overflow, software updates and patches, Browser knowledge, scripting, browser extensions, website knowledge, and honeypots
Network penetration & defense	Firewalls, port and IP scans and filtering, network knowledge, penetration testing, intrusion detection, big data analytics
Law & policy	Business impact analysis, disaster recovery, corporate email and account policy, privacy law and security policy
Physical security	Digital forensics, backup, and recovery
Virtualization	Virtual machines, and computer image
Personnel security & training	Security clearance, online references

nized the dynamic nature of cybersecurity. Thus, having a positive attitude in adopting new technology is essential. The participants also recognized the difficulties of "attribution" and "discernment" during cyberattacks as being "hard to figure out what the hackers are doing on your machine" (CD.14).

Progressive learning in cybersecurity is essential and knowledge of tools is built one upon another. Subject CD.02 progressed from Windows security to Linux security, eventually learning how to lure attackers to a honeypot, penetrating systems using Kali Linux, mapping network connectivity and topology, along with administering firewalls.

Learning to communicate was also crucial for cyber defense teams. Participants moved from one single physical system to multiple virtual machines that were running different services in a connected cloud environment. Participants also learned from trial and error. Subject CD.04 learned from observing other teammates' work, and also during personal time.

Learning takes place in many difficult venues. Subjects traditionally learn from textbooks and training sessions, as well as from their community (e.g., Cybersecurity Club), and online materials. Many different online sources were consulted in this process (e.g., Reddit, YouTube, Google, NIST, Dark Reading, etc.). Job training and internships were also a significant source of learning, as many participants learned from previous job experience in different contexts e.g., the military (CD.11), an engineering company (CD.10), desktop support in a healthcare setting (CD.12), a utility company (CD.13), as a data manager for a Children's Campaign (CD.05), app development in a software firm (CD. 06), and as a system integrator combining hardware components (CD.03).

5.2. *Cyber defense knowledge, activities, and tools*

Cyber defense tools are multi-faceted across several different domains. A total of nine (9) categories of tools and activities were identified from the interview transcripts (Table 1).

It's important to note that law and policy were viewed as an activity/tool by the cyber defense team. Institutional policy was also recognized as playing an essential role in protecting privacy and data confidentiality (CD.06). Subject CD.09 was aware of the "regulations for health informatics."

5.3. *Information protection and computer incident response as objects*

The object of the cyber defense teams was centered on protecting their information, systems, and networks and handling and responding to computer incidents and cyberattacks. The outcome of the object was divided into two categories within our coding scheme: achieved or not achieved. Most participants were pleased with the teamwork, as subject CD.10 said, "we did very good making sure the 'i's' were dotted and the 't's' were crossed." When the individual's objectives were aligned with the team's objectives, the team experienced positive learning outcomes. However, subject CD.10 also experienced frustration with one member of the team, complaining that "he didn't want to do anything."

Some participants experienced an inability to configure systems the way they hoped because they were "incredible amateurs at this, our front line is most likely going to have a lot of holes in it" (CD.15). As team members expressed their concerns and worries about the team not meeting their overall objectives, they began to grow from their existing individual activity system into a more encompassing collective activity system. These individual concerns serve as drivers for transforming the team's dynamics and operations as members began to grow out-of-the-box of their own individual activity system, to collective activity systems where members acquire rules, interact with other members on the team, stretch out in new directions and extend their reach to the community outside their existing circle.

5.4. *Code of conduct as rules*

Through the technical assignment instructions, each team began to ask questions among themselves and to search useful resources (either online or via access to personal acquaintances in the community). For example, subject CD.06 said, "when we did this lab, it was more for the requirements." The lab exercises instructed not only how the technology works, but also offered opportunities for the group to make decisions consensually.

Certain codes of conduct gradually developed within the team. For example, subject CD.02 expressed an internaliza-

tion of ethical behaviors, "don't steal what someone else has done, and I guess don't copy someone else's setup. Do it on your own."

5.5. *Leadership quality and management structure as divisions of labor*

Diversified talents and divisions of labor were also observed. Subject CD.06 stated, "my group members have a variety of knowledge in different areas." During computer incident response, subject CD.11 observed any problems or any change to the systems that you may have, you have to send that out and report them. This is what we are tracking. It's kind of an outgoing process; you have to have a lot of commitment to be in that position.

We observed ten (10) different leadership styles displayed during the team's interaction, which were also captured in the interview transcripts. Multiple leadership styles were observed during the team's computer incident response activities, which validates the leadership quality required for a cyber defense team to succeed in handling computer incidents.

1 **Assertive**. Several participants "took charge" (CD.10, CD.11, CD.13) and "stepped up" (CD.07, CD.09, CD.14).
2 **Coach**. Subject CD.10 also "made sure that my group understood what was needed," "I did a lot of the checks and balances on the side."
3 **Decentralized**. We observed that the subject, "stepped back" at times, and would "let people do what they wanted to do" (CD.10).
4 **Centralized**. "Having a captain" (CD.02) helped pull the team together.
5 **Democratic**. Teams operate based on group consensus with no specific leadership (CD.04). "the majority of the decisions was made—kind of a democratic process" (CD.06). Eventually, the team "all figured it out together" (CD.15).
6 **Hands-off**. From time to time, "leaders" would "step back and let people do what they wanted to do" (CD.10).
7 **Informal**. In the cyber defense team, "that person just kind of naturally rose to the task" (CD.02). Sometimes, the team leader was "not defined, but it was there" in the team (CD.15).
8 **Manipulative**. Occasionally, the manipulative style surfaces in the team's interaction. For example, subject CD.10 asserted his personal preference, "No… this is how you do it."
9 **Performance-driven**. Almost all leaders were performance-driven. For example, subject CD.06 said, "just making sure everyone else is on their stuff, so I kind of set up that role that, hey this is coming up. General reminders and stuff like that." Subject CD.10 "made sure that everything was followed. Everything was on point that needed to be done." And subject CD.13 "made sure that everything is going to be/ get turned in on time."
10 **Silent**. We observed that one participant had domain knowledge but decided not to convey best practices to the group. The participant did not want to intimidate other group members with his prior/superior experience (CD.06). Another subject described himself saying "I am guessing my role would be a silent leader that was just on the side" (CD.10). We observed a similar struggle from subject CD.11 that said, "In that sense, I would say that I am the leader of the group, but I don't want to, I don't want to label myself as the leader of the group."

Technical expertise is expressed in leadership. Those who have the technical expertise tended to take on a leadership role. As subject CD.06 explained, "that was kind of why you took that leadership role because you had some experience there." Subject CD.09 stated, it "was half necessity, half self-employment… I was the only person with previous experience using those systems, so I had to sort of step up and lead the way." Subject CD.15 agreed, "He seemed to have a better grasp on things than we did."

Both top-down, as well as bottom-up approaches, were observed from the team's interaction and management during cybersecurity operations. Subject CD.04 depicted top-down delegation as "we try to delegate based on ability rather than just whoever." Subject CD.07 stated that "pretty much I'll lay out exactly what we need to do, assign them their certain parts of the paper. Once they have everything completed, I try to get us all together and mesh them orderly." However, "leaders evolve over time," as subject CD.02 expounded. Grassroots effort from the bottom-up is commonly observed among cyber defense teams. "Everyone contributes ideas," (CD.02). Subject CD.06 also revealed that as far as the division of labor, it "naturally evolved; no structure." "Co-leadership," as suggested by subject CD.14, "is pretty much how the team operates." There were no defined roles, but "we would layout the problems and tackle it as a team," (CD.15).

We also observed five (5) coordination practices displayed in the team's interaction. This indicates that emotional frustration will be experienced if members of the team do not respond appropriately to each other. Team members expect each other's support in their coordination to solve problems.

1 **Coordinated** based on "group consensus" (CD.04).
2 **Frustrated** when one member of the team "did not want to do anything" (CD.10).
3 Everyone was expected to be **responsive**. The team made sure "everyone is caught up, up-to-date, knows what we are doing, and is able to move quickly when we have something come up" (CD.04). "When things had to get rolling, I was right there" (CD.10).
4 **Watchful** as subject CD.10 "did a lot of checks and balances."
5 **Communicative**. Subject CD.10 states that "I make sure I find a way to communicate."

Separation of duties determined how each team operated and was coordinated. For example,

> We probably have some people go through making sure the software is running properly. We could have some people doing some rudimentary testing, seeing if any of the biggest attacks work and making sure that none of them do. Some people actually going up researching whatever current attacks there are, there are more recent ones I should say and making sure those don't work as well. (CD.02)

Subject CD.04 stated that

> We usually have that one person do that one specific thing they are good at, because we try to delegate about ability rather than just whoever, if we can get the person who is best at say, Ubuntu, which is the actual server itself and the actual defense, that person will be going to Ubuntu. If we have someone who is really good at Kali and Linux, which is the offensive portion, he is going to Kali Linux and that is how we delegate it. If we have a fifth member who really doesn't have anything, we will set that person as support to provide additional service when needed. So, if a plan starts falling apart, we can have that extra manpower to help maybe bridge the gap.

5.6. *Circles of community*

Participants identified and formed their community of support. Their immediate community refers to their teammates, peers, and friends. Then, the next circles of support include the IT Helpdesk and online resources and connections. Subject CD.13 said, "Google anything that you have. If you are thinking of it, there is somebody online that probably thought of it too and got some response on it." The third circle of the community includes the open-source community and related professional groups. Subject CD.05 referred to the open-source community as "an online technology community. Usually, it is basically a community of information professionals." Participants would post questions to online communities such as Spiceworks or Stack Exchange. For example, subject CD.06 mentioned, "some organizations are out there that deal with just sharing intel and information so that everyone is able to speed up." The importance of circles of community tends to increase as these young adults progress to become cyber information professionals Ho (2020).

6. Cyber defense as a sociotechnical activity system

Unlike other theories, activity theory is mainly concerned with being able to describe and understand an activity, rather than to predict human behavior [(Nardi and Nardi, 1996), p. 4]. The cyber defense activity system below explicates the influences that mediate participants' development in completing the assignment and moving toward the projected outcome of developing a consciousness of cyber defense that will allow them to protect information assets and cyberinfrastructure. This development is experienced at both an individual and a collective level. The diagram demonstrates the relationships between the various nodes in the activity model using arrows and describes how the relationships between the nodes affect the attainment of the object and ultimately the desired outcome.

6.1. *Individual learning activity systems*

The four triads of individual-level activity learning systems were observed (Fig. 3). The arrows within imply the direction of learning.

6.1.1. *First learning system—subject, activity/tools, and object*

The relationship between the subject, the activity being performed, and the object are primary to understanding the behaviors that are taking place. The subject, conceptualized as either individuals or as the teams, has to have a motivation for their actions. That motivation is often the desire to obtain a goal, called an object. For example, participants can be motivated by the desire to solve a technical problem during a computer incident response task or to demonstrate their expertise. The tools the subject uses to move toward the object will be affected by the conditions in which the activity is being undertaken. Conditions and motivations can change, and these, in turn, can alter the activities undertaken, or even the object sought. The object, in this case, is to protect the system and respond to computer incidents. Participants learn a variety of security systems and mechanisms, as well as develop knowledge, skills, and behaviors that facilitate reaching that object.

6.1.2. *Second learning system—community, division of labor and object*

The relationship between community, division of labor, and the object is very focused on the decisions made by members within a team. Team members have to decide how they are going to work together, and the extent to which they want to collaborate and assign roles or work independently. Collaboration is a favored strategy for success. The data in this study revealed a hesitancy to assign leadership positions and a tendency to assign roles based on team members' technical expertise. The power of personality and/or technical expertise sometimes allowed leaders within a group to emerge, but overall participants worked within a fairly democratic process, looking to the team to assign roles and make decisions together. The relationship between community, division of labor, and the achievement of the object can also be affected by the sense of responsibility assumed by individuals toward the successful attainment of the object.

6.1.3. *Third learning system—subject, rules, and community*

The relationship of subject, rules, and community can somewhat be portrayed as the social context of the activity. The teams experienced a variety of stakeholders in their success within the communities they encountered. The immediate community was the cyber exercise context set for the class including the instructor and their peers. The class was embedded in a larger program of study within a school, within a college, within a university. Their classroom experience was primarily a place to learn the rules, as provided by the assignment and class lectures and as agreed upon within their teams. Participants also found community support and information about rules in the Cybersecurity Club, which many of them attended. At the Cybersecurity Club (2021), they learned new skills and knowledge, could compete in games like capture the flag, and listen to guest lectures by professionals in the field. Professionals in the field represent another expansive community where professional norms can be learned. Participants not only interacted with professionals who participated in school events but also maintained relationships with previous mentors, employers, and coworkers. They also

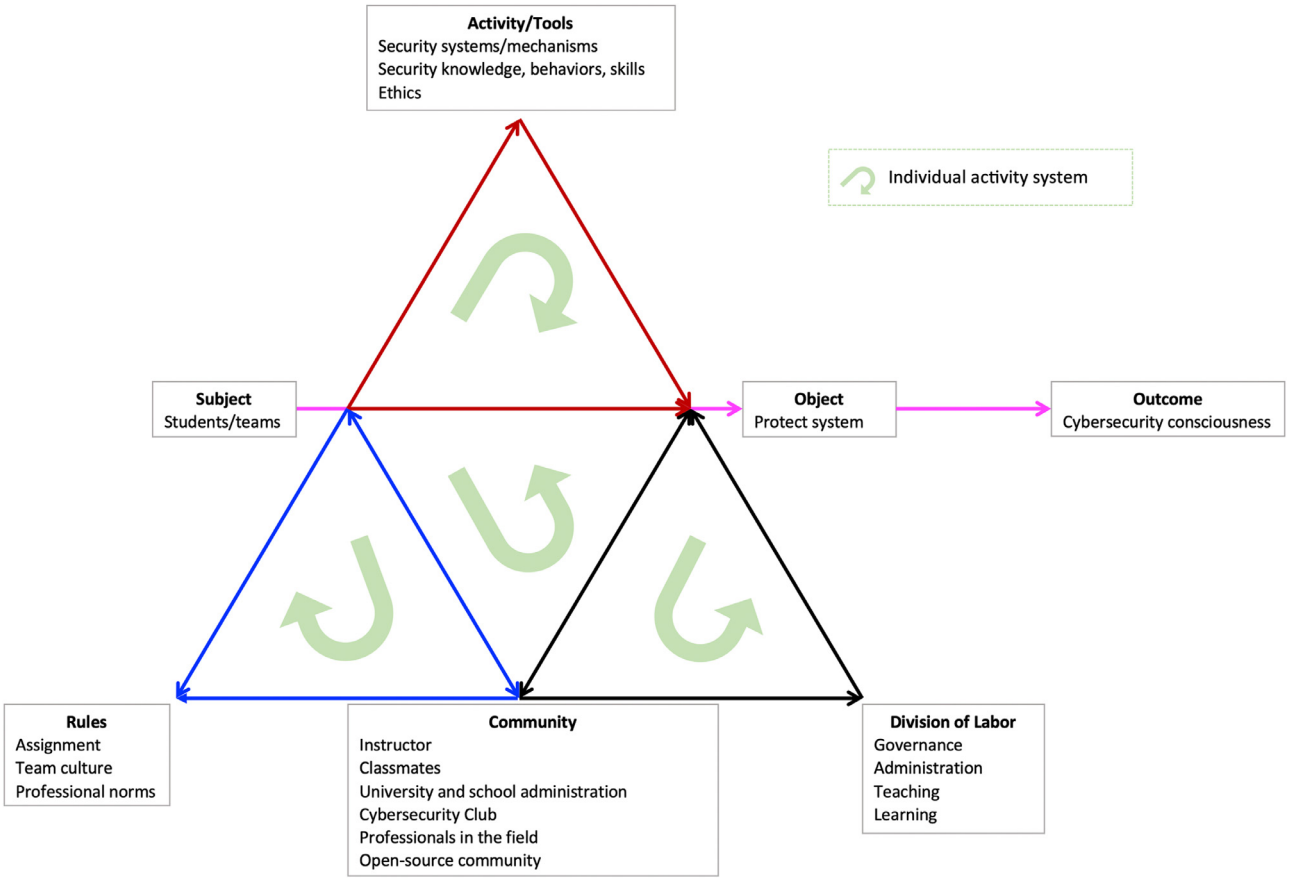

Fig. 3 – Four Individual Learning Activity Systems.

relied largely on the open-source community to build knowledge and skills and rules of the road. The circles of community substantiate and regulate the professional and ethical code of conduct for cyber defenders as well as cyber defense teams.

6.1.4. *Fourth learning system—subject, community, and object*

The relationship between the subject, the community, and the object, in this case, has to do with the various stakeholders' interest in the success of these participants. All layers of the community are vested in helping individuals achieve the object of protecting their system and the outcome of developing a professional consciousness of cyber defense. The triad of subject, community, and object is portrayed by the tacit knowledge and resourcefulness of the subjects in addressing and achieving the object. During computer incident response, the subjects reach out to the community and reference online resources (e.g., GitHub, Google, Common Vulnerabilities and Exposures (CVE), OWASP, YouTube videos, and many) to learn how to troubleshoot computer incidents and identify workarounds for solving problems. As subjects face more computer incidents, they tend to turn to the community for assistance and help.

6.2. *Collective learning activity system*

The collective activity system is multilayered, multi-relational, and involves all four triads and all relationships between components. The community governs professional norms, powers the tools, and gauges collective goals through an organic division of labor. The subject interacts with—and learns from—the community to reach the object. As a result, the subject takes collective actions to mature in problem-solving and technical trouble-shooting ability, reaching the consciousness of cyber defense as an intended outcome. The object of protecting information, systems, and networks is no longer *individually*-based, but a collective goal that involves not only the team and the organization, but the community at large.

More specifically, we observed three diagonals in the collective activity system. Each diagonal illustrates multi-layered intersections of two remote nodes with two directions in the collective model. First, community and activity are connected to indicate that the community can influence the activity performed and the tools employed (Fig. 4). The advice received in class, from the Cybersecurity Club (2021), via professional contacts, online references, and even from the open-source community can influence how the subjects seek the object.

Second, the two-directional arrow connecting rules to the object through the subject recognizes that rules can also affect how subjects go about achieving the object (Fig. 5). It indicates that professional norms and ethics, policies and procedures, and even laws practiced by the professional community can preclude certain undesired behaviors and advantage positive behaviors (e.g., ethical codes of conduct).

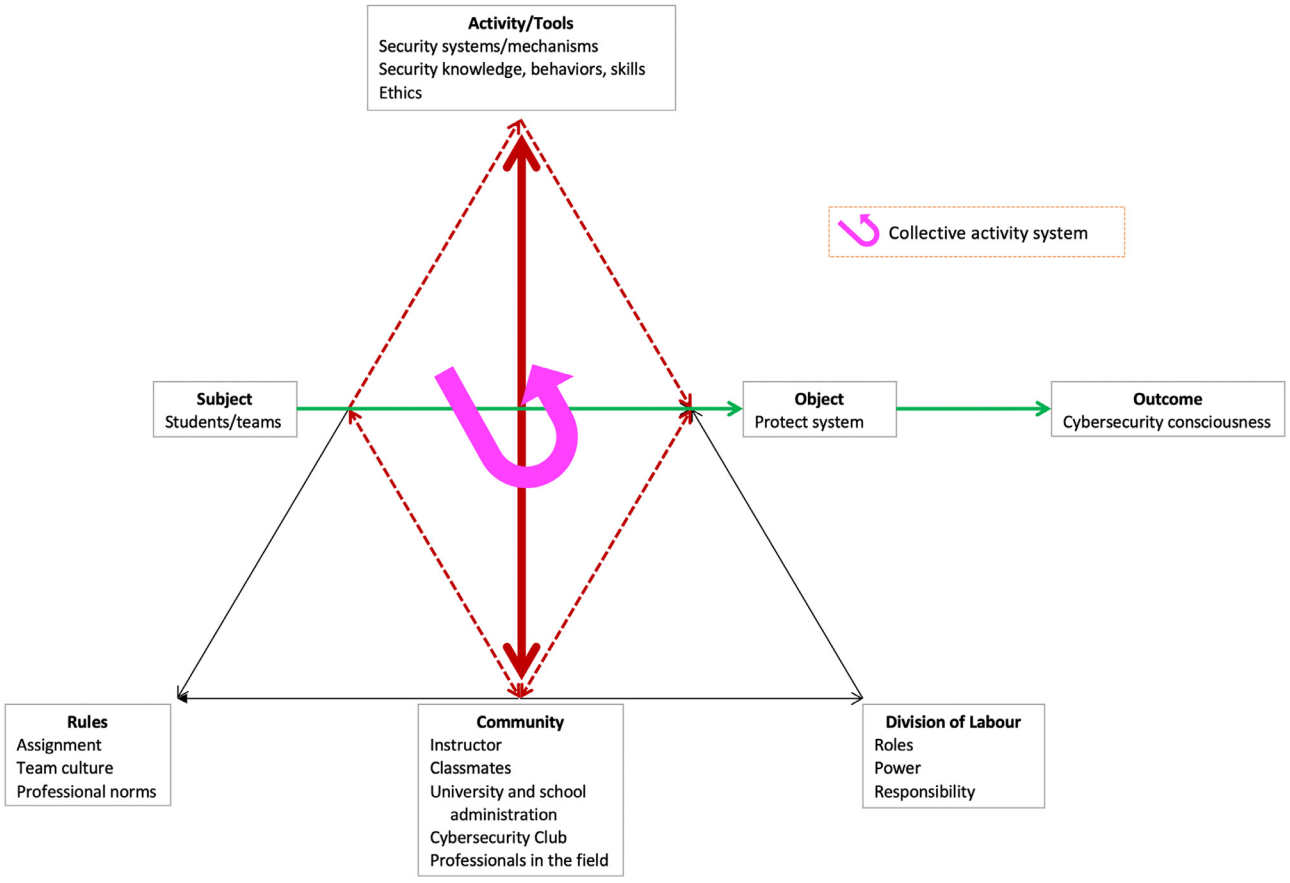

Fig. 4 – First Collective Learning Activity System.

The third direct diagonal connection is between the subject and the division of labor (Fig. 6). As noted above, the division of labor was largely in the hands of the teams themselves and developed throughout the assignment. As subjects developed skills to achieve the object of protecting systems and responding to computer incidents, this object determines how the team's management is structured and how the team coordinates based on members' initial differences in expertise, skills, and knowledge. The teams learn to collaborate autonomously according to leveraged differences and skillsets. The object of protecting systems bridges individual differences, and thus the teamwork became more sophisticated.

7. Discussion and implications

Use of the activity systems model and the framework of expansive learning produced a thick description of the development of a consciousness of cyber defense among students working in a cloud-based sandbox environment. The unit of analysis is the activity itself but recognizes that activity is mediated, guided, and influenced by factors that can be isolated and analyzed to understand the overall cyber defense system, which is highly dynamic. The participants who experienced this educational intervention, and shared their perceptions and experiences, provide a view of how learning outcomes can be achieved. The provision of a sandbox environment, in which activities could be undertaken without real-world consequences provided a safety net within which mistakes could be made, consequences experienced, and knowledge and skills internalized.

The resulting cyber defense activity systems have implications for both theory construction as well as pre-professional training and the analysis of workplace activities in organizations. While the findings describe the experiences of cyber defense teams engaged in computer incident response training, these findings can be translated to organizational transformation and learning.

7.1. *Theoretical implications*

Regarding incident response teams, Brown et al. (2016) borrowed the internationalization/externalization concepts from activity theory to explain the workflow among these teams and identify gaps between standards and the actual response work in Security Operations Centers (SOCs). Nyre-Yu et al. (2019) also adopted an ethnographic approach to observe how CSIRTs work while emphasizing the criticality of context-awareness in cyber defense operations. There is no doubt that we can gain rich insights from an ethnographic approach to incident response and handling using an authentic organizational setting. For example, Bartnes et al. (2016) conducted a case study from within electrical power companies and McLaughlin et al. (2017) interviewed industry players

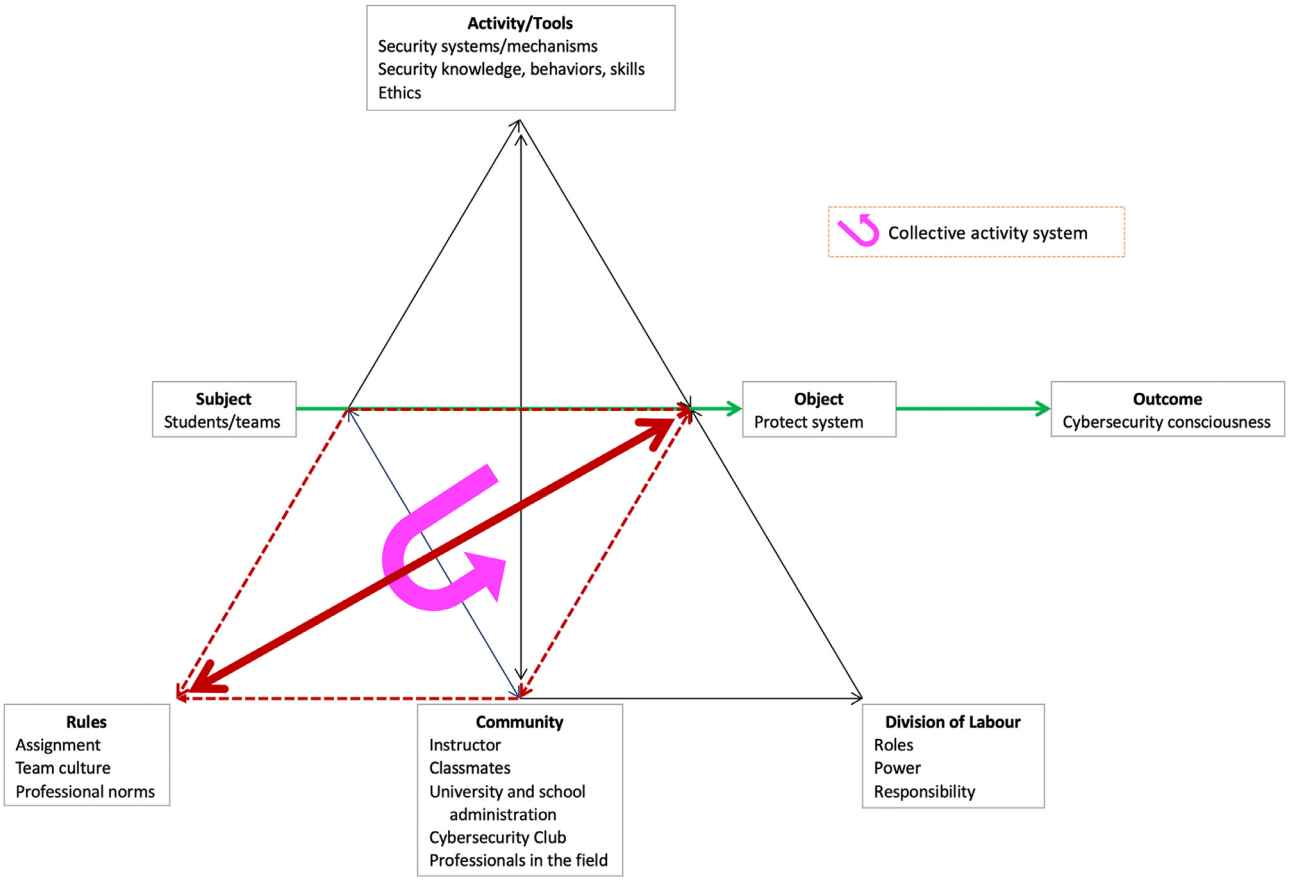

Fig. 5 – Second Collective Learning Activity System.

to identify characteristics and skills of incident responders. However, the use of cyber labs as seen in Topham, Kifayat *et al.* (Topham et al., 2016) and experimental design allows us the opportunity to discover transferable findings and identify both individual learning mechanisms and organizational collective learning mechanisms as contributions to cyber defense operations and organizational cyber awareness.

The process of mapping cyber defense activity to organizational contexts is necessary to reveal the full utility of the model for training cybersecurity professionals and thinking about how cyber defense activities are undertaken in organizations. The analysis of each of the nodes in the model—as well as consideration of how the nodes influence each other—can reveal opportunities for manipulation of the activity as a way of reassessing why and how objectives are sought, or whether the rationale used to define the objective is correctly conceptualized.

One of the findings from our study that is prime for further investigation is the impact of the role of leadership, and the ways that leadership asserts itself in these teams. Many of the participants described themselves as leaders and yet, in almost every team no official leader was guiding the activity. Several different leadership styles emerged as the teams became more cohesive and built up their technical skills and knowledge. The role of leadership in successful cyber defense teams remains an open question. In most organizational contexts, leadership is defined in the organizational chart and assigned through hiring practices. However, an individual's leadership ability may be a factor associated with effectiveness. Future research on cyber defense can assess the advantages and disadvantages of a leaderless team versus a single team leader, or a particular style of leadership and explore the question of whether the ability to lead—formally or informally—is an important characteristic for cybersecurity professionals.

Motivation is an important kingpin for any activity. If there is no motivation to achieve the object, it is unlikely that the activity will be engaged in. When the subjects are motivated, the driving force behind their actions will determine their behavior and may result in changes to the objective sought. Participants in the study were interested in obtaining advanced knowledge and skills that would prepare them for handling computer incidents and the need to protect their systems. Motivations for cybersecurity professionals are likely slightly different in the field, but similar desires, such as a paycheck—or the ability to display expertise—may play a role. Investigations into the function of motivation in maintaining the cyber defense objective would be interesting to explore.

There are several ways the concept of community supports and informs the cyber defense objective. The first level of community is the team structure that built alliances between individuals. These relationships were important, but the success of the team is also bolstered by the clear objectives of an organization's management. Additional community support includes a variety of connections to professionals in the

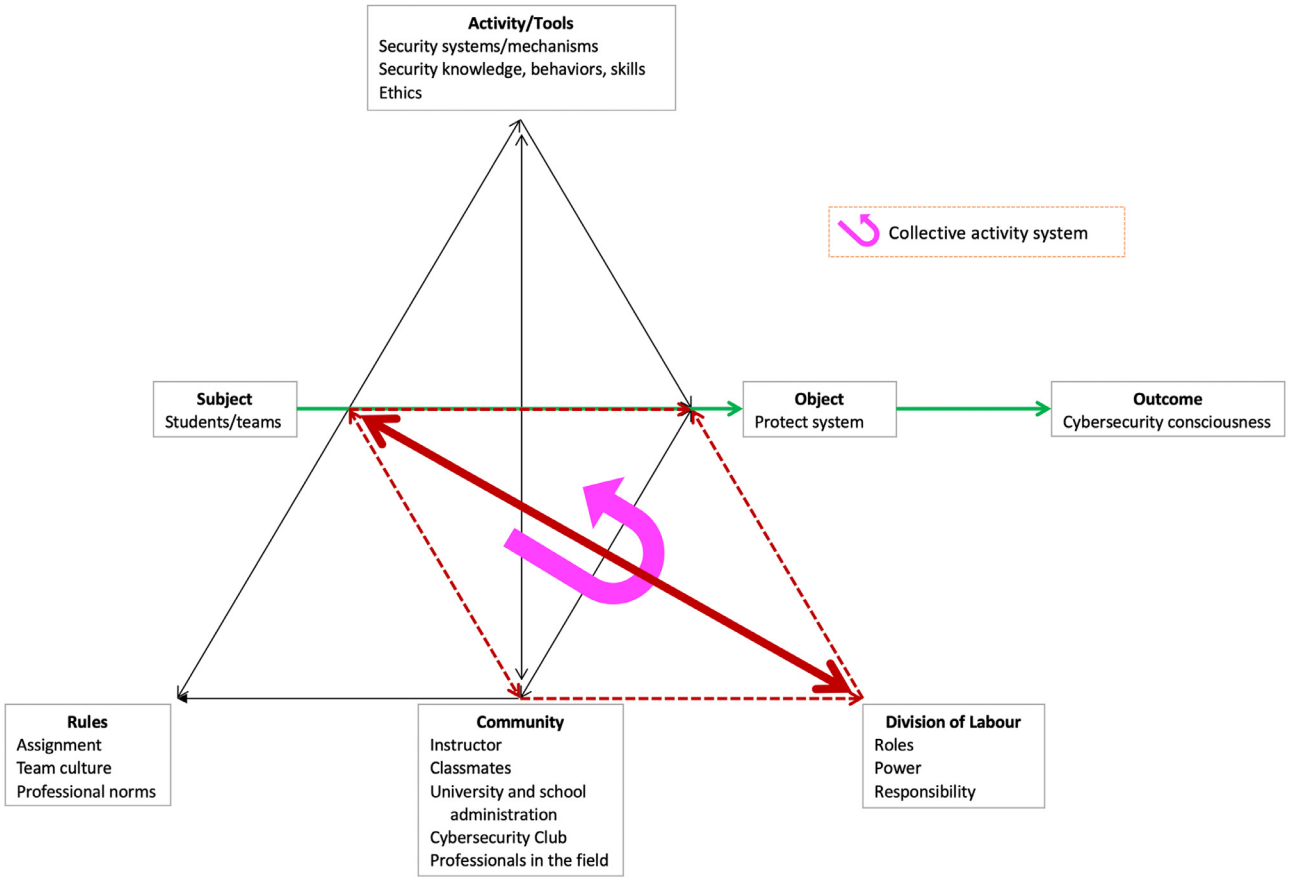

Fig. 6 – Third Collective Learning Activity Systems.

field as well as in the open-source community. All of these relationships represent important intersections between individual learning and the collective activity system where support, professional norms, rules, and ethics also influence motivations, activities, and objects. The expression of community for cybersecurity professionals in the workplace may be a concern for organizations, as cyber defense is a goal that inevitably supersedes the interests of any single individual. The question of how community is experienced and affects activity in the workplace—and the consciousness of cyber defense among employees—is another interesting research topic to be pursued.

Lastly, the efficient division of labor is a topic that will benefit from more investigation. In an organizational context, the support of expansive learning for the cyber defense team is essential. Individual subjects need the opportunity to learn a variety of tools and to take on more than one role in the team structure. As teams grow in expertise and the cloud environment becomes more complex, some individuals may be motivated to learn more and adapt quickly. Other individuals may wish to rely on skills they have already mastered and roles that are in their comfort zone, not necessarily because this is easier, but as a way to make their team more competitive. These dynamics of the division of labor are likely to exist in most organizations. The division of labor has multiple consequences and should be strategic in a way that promotes individual growth as well as the attainment of the cyber defense objective.

7.2. *Practical implications*

The study has several takeaways for management with regards to building an in-house cyber defense team within the organization.

Subject. Cyber defenders should have technical expertise in the tools and systems, along with proficient communication skills and orientation as a team player. This is consistent with findings from Dawson and Thomson (2018) who emphasized the need for not only systems knowledge but also a team player mentality, and Crumpler and Lewis (2019) who support the need for both technical and social skills. Individual concerns can be a driver for building team dynamics. Organizations can promote these traits among existing employees, and look for these traits in candidates during the hiring process.

Activity. The activity undertaken as expressed in the use of specific knowledge, tools, and/or skills is of particular importance in a field where mastery of these fundamentals is an unending process. The proliferation of technologies and human ingenuity in devising new lines of attack negates the idea that knowledge in this field can ever be fully attained. Almost any tool represents a double-edged sword, and over-reliance on existing systems and mechanisms can be a trap. A

viable cyber defense team requires a wide range of knowledge, skills, and tools. Continuous learning must be a requirement for professional cyber defenders, and organizations must support this professional development.

Object. There are both short-term and long-term objectives for cyber defense. Short-term objectives include handling and responding to computer incidents—whereas long-term objectives include protecting information, systems, and the networked environment—whether virtual or physical. However, these objectives are dynamically changing due to the wide variety of computer incidents, which may have an impact on the motivation of cyber defenders as they shift between activities and tools. The relationship between the cyber defenders (subjects) and objectives (objects) is dynamically mapped and may mutate based on the evolution of computer incidents. Organizations should make these goals and objectives clear to the cyber defense team and ensure that the team remains on track.

Division of Labor. Division of labor tends to result from the evolution of established skills, knowledge, and experience. It is important to provide advanced opportunities for progressive learning while promoting a culture of continuous learning (Ho et al., 2017).

Rules. Organizations are required to implement policies and procedures to detect, contain and correct security violations. Moreover, computer incident response practices and process should also be regulated (Grispos et al., 2015). Within the structure of the organizational policy and procedure, team culture will develop its own unique guidelines for efficient operations. The inflexibility of imposed rules can affect the timeliness of handling and response to a computer incident. A clear organizational policy for information privacy and data protection is essential and equivalent in importance to the ethical code of conduct that is reinforced by the cyber defense professional community. Moreover, the adoption of incident response criteria—while helpful—should be examined for constraints within certain contexts to maximize its optimal outcome of incident learning and dissemination within the organization (Grispos et al., 2015).

Community. Cyber defenders need a strong community to keep their motivation aligned with goals. They tend to be people that value and maintain professional relationships. Sources of information and support are as important as continuous and just-in-time learning.

Computer incidents are often viewed as problems and contradictions that manifest within the organization. While problem-solving skills and the adaptability of the cyber defense team are essential, it is even more vital to recognize the importance of responding to and handling computer incidents. These contradictions are necessary for the ongoing development of the organization. Examining and solving the contradictions can provide important insights for understanding organizational change (Allen et al., 2011; Kuutti, 1995; Ho et al., 2019). Organizations should view computer incidents (contradictions) as opportunities to grow and transform into a more secure virtual organization.

7.3. *Study limitations*

Activity theory is unique in that its strength is in providing a deep description of behavior. However, activity theory is weak in terms of its ability to make predictions. The choice of theory is like choosing a pair of glasses and should be selected for its ability to address the research question. Activity theory was employed throughout this study to take advantage of its descriptive ability to help us consider specific aspects of behavior in the context of a sandbox experiment. Choice of a different theoretical framework is unlikely to produce identical findings and should be considered in future work.

This study involved a small sample—as is common in qualitative studies Miles and Huberman (1994). Findings from this study express the perceptions and experiences of specific participants reflecting on their involvement in laboratory experiments. Without further research, we will not know the extent to which the data may be transferable. While the sandbox design helped tease out specific variables important in activity theory, future work can apply the theory to real-world incidents within specific organizational environments looking at organizational factors.

8. Conclusion and contribution

Cyber defense has been conceptualized and operationalized as a collective activity, where multiple individuals are grouped into cyber defense teams and participate in taking actions to transform the organization. In responding to computer incidents, cyber defense teams take actions not only to address their objects in protecting their systems, but also to transform the organization collectively into a more secure environment.

The cloud-based sandbox laboratory environment simulates real-world cyber defense and cyber-attack scenarios where 'offensive defense' is exercised and deployed. This affords individuals hands-on experience with opportunities to respond to computer incidents, further facilitating a team-based consciousness for cyber defense. This novel collective learning system is efficacious in developing the consciousness of cyber defense while informing further development and use of activity theory in the study of cyber defense. In addition to the four individual learning activity systems, this study identifies three collective learning activity systems that provide novel insights and mechanisms for organizations to increase their cyber awareness. Through hands-on engagement and teamwork while responding to computer incidents, organizations gain collective experience, knowledge, and skills, which are thus transformed. More importantly, cyber defense consciousness gained by organizations will prepare them for future cyber threats.

Author contribution

Conception and design of study: S.M. Ho

Acquisition of data: S.M. Ho

Analysis and/or interpretation of data: S.M. Ho & M. Gross

Drafting the manuscript: S.M. Ho & M. Gross

Revising the manuscript critically for important intellectual content: S.M. Ho

Approval of the version of the manuscript to be published (the names of all authors must be listed): S.M. Ho & M. Gross

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors wish to thank Alison von Eberstein for the contribution on the interview/survey questionnaire, participant informed consent form, and the Institutional Review Board (IRB) protocol approved by Florida State University Human Subjects Committee. The authors also wish to thank Christy Chatmon for the effort on interviewing participants and data collection during Spring 2017, Vanessa Myron for the effort on transcribing interviews, and Sushmita Khan for teh effort on interview data analysis during Fall 2018.

REFERENCES

Ahmad A, et al. Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput. Security 2019;86:402–18.

Ahmad A, et al. How integration of cyber security management and incident response enables organizational learning. J. Ass. Inform. Sci. Technol. 2020;71(8):939–53.

Ahmad A, et al. How can organizations develop situation awareness for incident response: A case study of management practice. Comput. Security 2021;101.

Ahmad A, Hadgkiss J, Rulghaver AB. Incident response teams – challenges in supporting the organisational security function. Comput. Security 2012;31(5):643–52.

Ahmad A, Maynard SB, Shanks G. A case analysis of information systems and security incident responses. Int. J. Inf. Manage. 2015;35(6):717–23.

Allen D, Karanasios S, Slavova M. Working with activity theory: context, technology and information behavior. J. Am. Soc. Inform. Sci. Technol. 2011;62(4):776–88.

Bartnes M, Moe NB, Heegaard PE. The future of information security incident management training: a case study of electrical power companies. Comput. Security 2016;61:32–45.

Baskerville RL, Spagnoletti P, Kim J. Incident-centered information security: managing a strategic balance between prevention and response. Inform. Manage. 2014;51:138–51.

BBC. US Cyber-Attack: US Energy Department Confirms it was hit by Sunburst Hack. BBC News; 2020. 2020 December 18Available from https://www.bbc.com/news/world-us-canada-55358332 .

Bing C. Suspected Russian Hackers Spied on U.S. Treasury Emails - Sources. Reuters; 2020. 2020 December 13Available from: https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUSKBN28N0PG.

Bodea C-N, Dascalu M-I, Cazacu M. Increasing the effectiveness of the cybersecurity teaching and learning by applying activity theory and narrative research. Issues Inform. Syst. 2019;20(3):186–93.

Bostrom RP, Heinen JS. MIS problems and failtures: a socio-technical perspective. Part II: The application of socio-technical theory. MIS Q. 1977;1(4):11–28.

Bostrom RP, Heinen JS. MIS problems and failtures: A socio-technical perspective. Part I: The causes. MIS Q. 1977;1(3):17–32.

Brown JM, Greenspan S, Biddle R. Incident response teams in IT operations ceters: the T-TOCs model of team functionality. Cogn. Technol. Work 2016;18:695–716.

Chambliss WJ. State-organized crime. Criminology 1988;27(2):183–208.

Chen R, et al. Design principles for critical incident response systems. Inform. Syste. e-Bus. Manage. 2007;5:201–27.

Chen R, et al. Data model development for fire related extreme events: an activity theory approach. MIS Q. 2013;37(1):125–47.

Cohen Z, et al. US Cybersecurity Agency Warns Suspected Russian Hacking Campaign Broader than Previously Believed. CNN; 2020. 2020 December 18Available from https://www.cnn.com/2020/12/17/politics/us-government-hack-extends-beyond-solarwinds/index.html .

Cole M, Engeström Y. A cultural-historical approach to distributed cognition. In: Salomon G, editor. In: Distributed Cognitions: Psychological and Educational Considerations. Cambridge, MA: MIT Press; 2001. p. 1–46 Editor.

Cooke D, Rohleder TR. Learning from incidents: from normal accidents to high reliability. Syst. Dynamics Rev. 2006;22(3):213–39.

Crumpler W, Lewis JA. In: The Cybersecurity Workforce Gap. Center for Strategic & International Studies (CSIS); 2019. p. 1–10.

Cybersecurity Club at Florida State University. n.d. [cited May 5, 2021]; Available from: https://cybersecurity.fsu.edu/club/.

Dawson J, Thomson R. The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Front. Psychol. 2018;9:1–12.

Diaz J. Russia Suspected in Major Cyberattack on U.S. Government Departments. NPR; 2020. 2020 December 14Available from: https://www.npr.org/2020/12/14/946163194/russia-suspected-in-months-long-cyber-attack-on-federal-agencies .

Drtil J. Impact of information security incidents: theory and reality. J. Syst. Interation 2013;4(1):44–52.

Dutton JE, Dukerich JM. Keep an eye on the mirror: Image and identity in organizational adaptation. Acad. Manag. J. 1991;34(3):517–54.

Dutton JE, Dukerich JM, Harquail CV. Organizational images and member identification. Adm. Sci. Q. 1994;39(2):239–63.

Engeström Y. In: Learning by Expanding: An Activity-Theoretical Approach to Developmental Research. New York: Cambridge University Press; 1987. p. 338.

Engeström Y. *Where is a tool? Multiple meanings of artifacts in human activity*, in *Learning, Working and Imagining*. In: Engeström Y, editor. In: Painettu Kirjapaino Oma Ky: ssa, Jyvaskylassa; 1990. p. 170–93.

Engeström Y. In: Learning, Working and Imagining: Twelve Studies in Activity Theory. Helsinki: Orienta-Konsultit Oy; 1990. p. 293.

Engeström Y. 23 Innovative learning in work teams: Analyzing cycles of knowledge creation in practice. In: Engeström Y, Miettinen R, Punamäki-Gitai R-L, editors. In: Perspectives on Activity Theory. Cambridge, MA: Cambridge University Press; 1999. p. 377 Editors.

Engeström Y. Activity theory as a framework for analyzing and redesigning work. Ergonomics 2000;43(7):960–74.

Engeström Y. Expansive learning at work: Toward an activity theoretical reconceptualization. J. Education Work 2001;14(1):133–56.

Engeström Y. Enriching activity theory without shortcuts. Interact. Comput. 2008;20:256–9.

Engeström Y, Sannino A. Discursive manifestations of contradictions in organizational change efforts. J. Organ.Change Manage. 2011;24(3):368–87.
Fulton E, Lawrence C, Clouse S. White hats chasing black hats: Careers in IT and the skills required to get there. J. Inform. Syst. Education 2013;24(1):75–80.
Grispos, G., W.B. Glisson, and T. Storer, *Security incident response criteria: A practitioner's perspective*, in *The 21st Americas Conference on Information Systems (AMCIS 2015)*. 2015: Puerto Rico. pp. 1-11.
Gross M, Ho SM. Collective learning for developing cyber defense consciousness: an activity system analysis. J. Inform. Syst. Education 2021;32(1):65–76.
Handy, C., *Trust and the virtual organization*.Harvard Business Review, 1995: pp. 109.
Ho SM. Trustworthiness: top quality for cyber information professionals. In: Chang H-C, Hawamdeh S, editors. In: Cybersecurity for Information Professionals: Concepts and Applications. Boca Raton, FL: Auerbach Publications; 2020. p. 21–38 Editors.
Ho SM, Oliveira D, Rathi R. The shield and the sword: expanding learning in cyber defense through competition. Proceedings of the iConference 2019, 2019.
Ho SM, Oliveira D, Rathi R. Consciousness of cyber defense: boundary objects for expansive learning through creation of contradictions. In: Nah F, Siau K, editors. In: HCI in Business, Government and Organizations - Information Systems and Analytics. Springer Nature Switzerland AG; 2019. p. 338–53 Editors.
Ho SM, von Eberstein A, Chatmon C. Expansive learning in cyber defense: transformation of organizational information security culture. Proceedings of the 12th Annual Symposium on Information Assurance (ASIA'17), 2017.
Hove C, et al. Information security incident management: identified practice in large organizations. Proceedings of the 2014 Eighth International Conference on IT Security Incident Management & IT Forensics (IMF'14). IEEE Computer Society, 2014.
Iyamu T, Shaanika I. The use of activity theory to guide information systems research. Education Inform. Technol. 2019;24:165–80.
Kaptelinin V. Computer-mediated activity: functional organs in social and developmental contexts. In: Nardi BA, editor. In: Context and Consciousness: Activity theory and human-computer interaction. Cambridge, Massachusetts: The MIT Press; 1996. p. 45–68 Editor.
Kaptelinin V. The object of activity: making sense of the sense-maker. Mind, Culture Act. 2005;12(1):4–18.
Karanasios S, Allen D. Activity theory in information systems research. Inform. Syst. J. Special Issue 2018;28(3):439–41.
Kurt MN, Yilmaz Y, Wang X. Distributed quickest detection of cyber-attacks in smart grid. IEEE Trans. Inform. Forensics Security 2018;13(8):2015–30.
Kuutti K. *Activity theory and its applications to information systems research and development*,. In: Nissen HE, Klein HK, Hirschheim R, editors. In: Information Systems Research: Contemporary Approaches And Emergent Traditions. Amsterdam, The Netherlands: Elsevier North-Holland, Inc.; 1991. p. 529–49 Editors.
Kuutti K. Activity thoery as a potential framework for human-computer interaction research. In: Nardi B, editor. In: Context and Consciousness: Activity Theory and Human Computer Interaction. Cambridge: MIT Press; 1995. p. 17–44 Editor.
Kuutti K. Activity theory, transformation of work, and information systems design. In: Engeström Y, Miettinen R, Punamäki-Gitai R-L, editors. In: Perspectives on Activity Theory. Cambridge, MA: Cambridge University Press; 1999. p. 360–76 Editors.
Kuutti K, Arvonen T. Identifying potential CSCW applications by means of activity theory concepts: A case example. Proceedings of the 1992 ACM conference on Computer-supported cooperative work (CSCW'92). Toronto, Ontario, Canada: ACM, 1992.
Larsen KRT, McInerney CR. Preparing to work in the virtual organization. Inform. Manage. 2002;39(6):445–56.
Leont'ev AN. Retsenzija na knigu: Basov M Ya Obschie Osnovy Pedologii [Book review: General Foundations of Pedology by M Ya Basov]. In: Basov MY, editor. In: Estestvoznanie i Marxism; 1929. p. 211–13 Editor(In Russian).
Leont'ev AN. The problem of activity in psychology. Soviet Psychol. 1974;13(2):4–33.
Leont'ev AN. The Problem of Activity and Psychology. In: Leont'ev AN, editor. In: Activity, Consciousness and Personality; 1978. p. 45–74 Editor.
Leont'ev AN. Activity and Consciousness. In: Leont'ev AN, editor. In: Activity, Consciousness and Personality; 1978. p. 75–95 Editor.
Liu GJ, Shah R, Schroeder RG. Linking work design to mass customization: A sociotechnical systems perspective. Decision Sci. 2006;37(4):519–45.
McLaughlin M-D, et al. Capabilites and skill configurations of information security incident responders. Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.
Miles MB, Huberman AM. Qualitative data analysis: An expanded sourcebook. 2nd edition. Sage Publications, Inc; 1994.
Mitropoulos S, Patsos D, Douligeris C. Incident response requirements for distributed security information management systems. Inform. Manage. Comput. Security 2007;15(3):226–40.
Mowshowitz A. Virtual organization. Commun. ACM 1997;40(9):30–7.
Mowshowitz A. On the theory of virtual organization. Systems Res. Behav. Sci. 2000;14(6):373–84.
Nardi B. Studying context: A comparison of activity theory, situated action models, and distributed cognition. In: Nardi B, editor. In: Context and Consciousness: Activity theory and human-computer interaction. Cambridge, Massachusetts: The MIT Press; 1996. p. 69–102 Editor.
Nardi B, Nardi B. Activity theory and human-computer interaction. In: Context and Consciousness. Cambridge, Massachusetts: The MIT Press; 1996. p. 7–16 Editor.
Nardi B, Nardi B. Context and Consciousness. In: Activity Theory and Human-Computer Interaction. Cambridge, Massachusetts: The MIT Press; 1996. p. 1–400 Editor.
Nyre-Yu M, Gutzwiller RS, Caldwell BS. Observing cyber security incident response: Qualitative themes from field research. Proceedings of the Human Factors and Ergonomics Society 2019 Annual Meeting. Human Factors and Ergonomics Society, 2019.
Peckham R. Economies of contagion: financial crisis and pandemic. J. Econ. Soc. 2013;42(2):226–48.
Prapinpongsadorn S, Suwannatthachot P, Vicheanpanya J. Building a learning community among faculty, librarians and students using computer-supported collaborative learning: An activity theory approach. Proceedings of the 2017 IEEE 9th International Conference on Engineering Education (ICEED. Kanazawa, Japan: IEEE, 2017.
Ruefle R, et al. Computer security incident response team development and evolution. IEEE Security Privacy 2014;12(5):16–26.
Sanger DE. Russian Hackers Broke Into Federal Agencies, US Officials Suspect. The New York Times; 2020. 2020 December 13Available from

https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html .
Sawyer S, Jarrahi MH. Sociotechnical approaches to the study of information systems. In: Topi H, Tucker A, editors. In: Computing Handbook: Information Systems and Information Technology. Boca Raton, FL: Chapman and Hall/CRC; 2014. p. 1–27 Editors.
Schneider FB. Cybersecurity education in Universities. IEEE Security Privacy 2013;11(4):3–4.
Spasser MA. Informing information science: The case for activity theory. J. Am. Soc. Inform. Sci. Technol. Special issue (part 2) on Paradigms, Models Methods Inform. Sci. 2000;50(12):1136–8.
Suchman LA. In: Plans and Situated Actions: The Problem of Human Machine Communication. Cambridge University Press; 1987. p. 203.
Topham L, et al. Cyber security teaching and learning laboratories: a survey. Inform. Security 2016;35(1):51–80.
Trist EL, Bamforth KW. Some social and psychological consequences of the Longwall method of coal-getting. Human Relations 1951;4:3–38.
Vygotsky LS. Interaction between learning and development. In: Gauvain, Cole, editors. In: Mind and Society. Cambridge, MA: Harvard University Press; 1978. p. 79–91 Editors.
Wiesenfeld BM, Raghuram S, Galletta D. Communication patterns as determinants of organizational identification in a virtual organization. J. Comput. Virol. Hacking Tech. 2006;3(4):14.
Wiesenfeld BM, Raghuram S, Garud R. Communication patterns as determinants of organizational identification in a virtual organization. Organ. Sci. 1999;10(6):777–90.

Shuyuan Mary Ho is an associate professor at School of Information, at Florida State University. Her research focuses on trusted human computer interaction, including computermediated deception, cyberbullying, cloud forensics, cyber defense education, and sociotechnical 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*. Shuyuan is designated a 2021 Trusted CI fellow by *The NSF Cybersecurity Center of Excellence*, and her work has been funded by NSF and *Florida Center for Cybersecurity*, and featured in the popular press, e.g., *NPR, WIRED, Forensic Magazine*.

Melissa Gross is a professor in the School of Information at Florida State University and Past President of the Association for Library and Information Science Education (ALISE). She received her Ph.D. in Library and Information Science from the University of California, Los Angeles in 1998, received the prestigious American Association of University Women Recognition Award for Emerging Scholars in 2001, and in 2019 received the ALISE Award for Professional Contribution to Library & Information Science Education. Dr. Gross teaches and researches in the areas of information-seeking behavior, information literacy, library program and service evaluation, and information resources for youth. She has published extensively in a variety of peer-reviewed journals including *College & Research Libraries, Library & Information Science Research, Library Quarterly,* and the *Journal of the Association for Information Science & Technology*. She has authored, co-authored, or co-edited twelve 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).