Simulating Municipal Cybersecurity Incidents: Recommendations from Expert Interviews

Kira Gedris
Brigham Young University
kira.gedris@gmail.com

Kayla Bowman
Brigham Young University
kaylabowman2@gmail.com

Aatish Neupane
Brigham Young University
aatishnn@gmail.com

Amanda Lee Hughes
Brigham Young University
amanda_hughes@byu.edu

Elizabeth Bonsignore
University of Maryland
ebonsign@umd.edu

Ryan W. West
Brigham Young University
ryanwest6@gmail.com

Jon Balzotti
Brigham Young University
jonathan_balzotti@byu.edu

Derek L. Hansen
Brigham Young University
dlhansen@byu.edu

Abstract

As cyberattacks on city and public infrastructures become increasingly common and harmful, it is critical that we train the professional workforce to prepare and respond appropriately. This paper supports the development of educational simulations and related experiential learning exercises that help prepare city and public infrastructure personnel to effectively respond to cybersecurity attacks. Specifically, it synthesizes the findings from 8 expert interviews including 12 cybersecurity experts from federal, state, city organizations, as well as academics with relevant expertise. We organize the findings into key learning outcomes, scenarios, roles, and issues that simulation designers should consider. The result paints a vivid picture of the complex socio-technical context of city and public infrastructure attacks and responses and the most salient skills needed to respond to them.

1. Introduction

In this age of information, the hostages are not only people. In 2019, a ransomware attack in Baltimore demanded upwards of $76,000 USD to decrypt city data. The attack disrupted municipal systems to the point that the mayor proposed that employees clean city streets in lieu of office work [1]. Atlanta lost over $17 million recovering from a ransomware attack in 2018, which affected law enforcement and most other city services. Police officers wrote incident reports by hand when they were unable to access archived in-vehicle video [2]. Other cities, such as Kiev, have borne the brunt of cyberattacks that shut off the power grid and affected industrial control systems (ICSs) [3]. These attacks demonstrate the critical need to train city and public infrastructure professionals to prevent, prepare for, and respond to cyberattacks on cities and their public infrastructures. Indeed, most local governments report being less than confident in their ability to prevent similar breaches [4, 5].

Protecting a city against cybersecurity attacks is becoming more difficult. Unlike companies, city-wide infrastructure systems feature a fragile combination of heterogeneous systems with multiple stakeholders like government (local, state, federal) and private entities, and intertwined dependencies between them [6]. Due to these complex interdependencies, even a small localized attack can bring on a cascading series of failures that can compromise the city functions, and in some cases, even cost human lives. With the move towards smart cities and Internet of Things (IoT) devices, the challenge to defend against cyberattacks is even higher [7, 8].

Unfortunately, learning how to coordinate effectively and respond appropriately in such a complex, collaborative, and high-pressure situation is hard to do without actually experiencing the scenario. Since these scenarios are so infrequent and damaging, learning from experience alone is not a viable solution. This is one reason why educational simulations and experiential learning opportunities have grown in popularity among cybersecurity educators [9].

The goal of this paper is to support the development of educational simulations and related experiential learning exercises (e.g., games, tabletop experiences, competitions) that help prepare city and public infrastructure personnel to effectively respond to cyberattacks. Specifically, we synthesize the findings from expert interviews to identify key learning outcomes, scenarios, roles, and issues that simulation designers should consider. This work was conducted as background research for our own efforts to develop a city-wide cyberattack incident response simulation. However, we believe the insights we synthesize from expert interviews can inform different types of simulations and educational interventions.

URI: https://hdl.handle.net/10125/70862
978-0-9981331-4-0

2. Background

Cities and their critical infrastructures have become a major target of cyberattacks in recent years. These targeted cities have experienced data loss, theft, and other interruptions to normal operations, often spending millions on recovery efforts. Some attacks on cities and their infrastructures have been performed by nation states, such as the cyberattacks by Russian hackers in 2015 that shut off Ukraine's power grid [3, 10]. In recent years, international criminal gangs have used ransomware to make computing resources unavailable unless a significant bitcoin payment is made. The city of Atlanta was hit hard by ransomware in 2018. Fortunately, they recovered quickly because of the counter-strategy and manual operations they had in place which allowed them to keep water and emergency systems online during the attack [2]. Denver's Colorado Department of Transportation (CDoT) network was maliciously encrypted with malware when an unsecured web server was connected briefly to their network in 2018 [11]. They cleared their systems and restored backups, but failed to eradicate tools the hackers left behind, thus leaving their systems exposed. Baltimore's systems were exploited in 2019, resulting in a loss of critical city governance information where external backups were not in place. Billing, payments, and other transactions were frozen, incurring a loss of over $18 million in revenue and systems [12]. Attacks on cities are increasing in damage and frequency, highlighting the importance of countermeasures, backups, and cybersecurity training. Indeed, many municipalities are purchasing insurance to mitigate the potential damages incurred by such attacks [13].

Attacks on city and public infrastructures are particularly damaging. Many everyday activities that affect citizens' lives can be disrupted when public systems such as power, water, and transportation are affected. For example, cyberattacks that have led to physical damages include tram derailments in Poland (2008) [14] and the disruption of German steel mill operations (2014) [15], among others. Furthermore, municipalities maintain records with high levels of personally identifiable information (PII) that is a prime target for cybercriminals, including unique identifiers like driver's licence numbers. Successful attacks on such data lead to data exfiltration and theft, as well as embarrassment of individuals.

Securing city and public infrastructure is an extremely challenging job. City and public infrastructures host and integrate a variety of different devices, systems, and configurations ranging from standard IT systems to Industrial Control Systems (ICSs) including Supervisory Control and Data Acquisition (SCADA) systems that control physical equipment. Securing such disparate devices requires a wide range of expertise and coordination, as well as a good understanding of the interdependencies of different sub-systems. Another significant challenge is dealing with obsolete equipment such as outdated operating systems that are still needed to run legacy software that connects to ICSs [16]. City and public infrastructures are distributed among many stakeholders (e.g., city government, utilities, hospitals), with the need to provide security and integration across a range of organizations. Furthermore, general training in cybersecurity is often limited or non-existent [17]. Hiring personnel dedicated to cybersecurity can require taking funds from somewhere else, or raising taxes, both of which are less-than-ideal situations. Because training is also cut when local governments run low on funds [4], cybersecurity duties are often added to existing job responsibilities of IT staff, many of whom do not have sufficient training [18].

We need to prepare those who may work with city and public infrastructures to understand both the city environment and the cybersecurity risks associated with it. This is not only a technical problem, but a socio-technical one [19]. Almost 35% of security incidents are caused by human errors and negligence [20]. The Global State of Information Security Survey 2018 attributes 30% of security incidents as caused by current employees of organizations [21]. Often, those in non-technical roles unintentionally disclose information or allow physical breaches (e.g., lost, discarded, or stolen paper documents), which can lead to bigger threats [22]. Although there is a widespread mindset that cybersecurity is a responsibility of IT personnel rather than general employees [20], the problem is inherently collaborative – it cannot be solved by a single person or role. A functioning city consists of close-knit relationships between multiple government organizations and private entities working together [23]. Yet, 47% of IT professionals perceive a lack of collaboration between cybersecurity risk management roles and general organizational roles [20]. To ensure that coordinated response actions can be taken in the face of cyberattacks, it is essential that cybersecurity education stresses people's dependence on one another.

A variety of experiential learning activities have been used to help train cybersecurity students and professionals. For example, learners often work individually or in teams on cybersecurity competitions [24], simulations [25], games [26], tabletop exercises [27], and playable case studies [28]. These hands-on experiences allow learners to experience the stress of high-pressure, complex situations, while also providing a safe place for them to fail [29]. National CCDC and Cyberpatriot, two prominent cybersecurity competitions, allow teams of university and high school students, respectively, to test their defensive skills by protecting a small network from external threats. Anchored instruction suggests that interesting problems and engaging scenarios can form an "anchor" or context for students to use when trying to learn new skills and dispositions [30]. Consequently, simulations and related experiential learning activities have become an essential part of the fabric of cybersecurity education. Most of these experiences focus primarily on the technical aspects of cybersecurity, although there is recognition by the community that creating learning experiences that are more holistic and focused on social and cognitive aspects is important [25].

Researchers and educators have begun to explore and develop simulations that focus specifically on city and infrastructure cyberattacks. Frey et al. developed a LEGO based collaborative tabletop game about security in ICSs and human behavior in cybersecurity decision-making [31], with future plans to create a digital version. Play2Prepare, a board game for ICS security training with an objective to increase security awareness and encourage discussions during a security incident, also realized the need for a digital version to promote better team collaboration [32]. Another training program for municipalities is the tabletop exercise called a Jack Voltaic exercise that comprises different "Cyber Worst Day" scenarios to examine critical infrastructure interdependencies and encourage cross-sector information sharing. It also consists of a "Live-Fire Exercise" where cybersecurity equipment is capability tested in real time [33]. Additionally, classes that involve live, interactive simulations using real-world ICSs have been run at Idaho National Labs with professionals for years [34].

In addition to the explicitly educational simulations outlined above, developers have created test beds for ICSs (e.g., KYPO4INDUSTRY) that allow them to model the technical aspects of cyber-physical systems [35]. Most of these existing tools are either attack-specific or infrastructure-specific. Separate from particular types of attacks or scenarios, there have also been efforts to holistically consider interdependencies between critical city infrastructures [36], such as CIPMA, IIM, and NSRAM. CIPMA was designed as a decision-support system for the Australian Government to simulate complex interdependencies between critical infrastructure systems [37]. IIM is a computer-based simulation capable of simulating cascading effects of terrorist attacks on economic interdependencies [37]. The NSRAM is a network simulation tool that accurately considers the severity of network failures and repair variables (like time to repair, cost to replace, etc) [37]. While these systems currently serve operational purposes, they may one-day serve as a foundation for educational simulations.

Our hope is that a variety of new experiential learning interventions (e.g., simulations, games) will be developed that focus on protecting city and public infrastructure. This paper helps designers build upon a solid foundation of research-based learning outcomes and consider unique contextual factors.

3. Methods

To better understand potential learning outcomes, municipal cybersecurity attack scenarios, and other considerations for simulation designers and educators, we held interviews with a diverse group of 12 content experts between August and November of 2019. Our participants are established industry professionals and trainers focused on municipal cybersecurity from federal agencies and national labs, Computer Emergency Response Teams (CERT), municipalities, and corporations, as well as university professors with a background in cybersecurity and disaster response. Most interviewees have decades of experience in dealing with cybersecurity and have experienced or designed educational materials and/or simulations and tabletop exercises. This allowed them to provide expert advice on both the everyday experiences of those dealing with cyberattacks on city and public infrastructure, and the pedagogical issues of designing simulations. An ID for each interview (e.g., I-1) and a description of the attendees are included in Table 1. We refer to our interviews by number (e.g., I-1) to maintain anonymity.

Our immediate goal was to develop a realistic storyline and integrated learning activities for a new Playable Case Study (PCS) [38, 39] focused on a municipal cyberattack. However, we also saw this as an opportunity to ask questions broader than our project alone, so the findings could be shared with other simulation designers and educators. We performed semi-structured interviews [40], following an interview protocol that included broad questions about several topics including plausible cyberattack scenarios (e.g., types of attacks on cities), common work tasks (e.g., risk assessment strategies, processes for responding to cyberattacks), the people and roles involved in the work, key learning outcomes for junior cybersecurity professionals, helpful resources for novices, and concerns the experts had regarding future threats and vulnerabilities. We also explained our goal of developing a municipal cyberattack simulation, so interviewees could share advice and thoughts that would be useful for that context. All but two interviews were audio recorded and transcribed: these sessions were not recorded at the interviewees' request, but extensive notes were taken by multiple team members and integrated. Members of the team took detailed field notes during each interview session, then expanded upon these notes with first-round glosses of available audio recordings and qualitatively-coded interview transcripts.

We performed a thematic analysis [41] on the transcripts and field notes to identify themes in two key areas: learning outcomes and simulation design considerations. Four authors coded data. It began with two coders independently coding each interview transcript and set of notes, extracting important ideas and quotes that related to cyberattack simulations within each of the two key areas. Next, we did a second round to refine the coding scheme and consolidate coded passages across the two coders. We then discussed the resulting codes (and the quotes associated with them) and collaboratively and iteratively grouped them into the high-level themes presented in the paper. Themes were not determined a priori, but rather emerged through our analysis of the data.

Table 1. Interviews Conducted with Experts.

Interview ID	Description
I-1	Two cybersecurity trainers; two CERT content experts affiliated with a national lab
I-2	Professor studying skills/aptitudes of cybersecurity professionals
I-3	Professor & cybersecurity expert in federal government & industry
I-4	Professor with expertise in disaster response and cybersecurity
I-5	Security director for a major US city
I-6	Cybersecurity advisor in federal government; Information Security professional in industry
I-7	Emergency management lead in state government
I-8	Professor in CS with industry DNS/network security expertise

4. Results

4.1. Learning Outcomes

This section synthesizes the comments that experts provided about the most important knowledge, skills, and dispositions needed by those dealing with cyberattacks on municipalities. Table 2 summarizes the emergent themes and specific learning outcomes associated with each theme. The paragraphs that follow describe each theme, helping to tie them back to the specific comments made by interviewees.

4.1.1. Resourcefulness. Eight experts mentioned resourcefulness as one of the traits of a good cybersecurity professional. They spoke about how cybersecurity professionals should be able to acquire information from various sources and synthesize it to make informed recommendations for action. Experts talked about the importance of troubleshooting and searching for evidence (I-6), soliciting information from other departments (I-1), and networking with a community of peers to discuss recent threats (I-8).

4.1.2. Information Brokering. Another skill that eight of our experts agreed was important for cybersecurity professionals was an ability to communicate information to different audiences. One expert described that sometimes cybersecurity professionals are "not very good at communicating without being so in the weeds that nobody understands what they're doing" (I-5). I-6 described that cybersecurity professionals need to be comfortable with reporting on an event to company leadership. In addition to communication within one's organization, the expert in I-4 stated that communicating to the public is "a very pivotal role to any sort of crisis or disaster." Another interviewee emphasized what he considered "one of the big things in any incident, whether it's cyber or shooting or whatever, is communication of what's happened and what's being done. Those are all internal immediate communications" (I-7). This quote underscores how information brokering activities often occur in potentially stressful, real-time situations. Finally, several interviewees emphasized the importance of debrief reports and incident response plans, suggesting that writing clearly and using well-established cybersecurity report genres is an important part of information brokering.

4.1.3. Emotional Intelligence. Several traits that our experts (six) put forth as being the most important for cybersecurity professionals fell under the category of emotional intelligence. Our experts stated that those working in cybersecurity need to be patient during the

Table 2. Learning Outcomes for Professionals Dealing with Municipal Cybersecurity Attacks.

Theme	Learning Outcome
Resourcefulness	Acquire information, synthesize information from various sources, and make informed recommendations for action.
Information Brokering	Act as an information broker by translating and presenting technical concepts to non-technical audiences to bridge the gap between stakeholders (IT personnel, non-IT personnel, general public).
Emotional Intelligence	Develop patience and curiosity essential for stressful cybersecurity scenarios. Understand how people in different roles think.
Holistic Approach	Assess risk and higher-order effects from multiple perspectives, and build a comprehensive vision from the various pieces.
Preparation	Understand the importance of preparation, following best practices, prioritizing important decisions ahead of time, and put in place proactive measures to protect systems.
Cybersecurity Awareness	Understand the importance of security awareness at all levels and be aware of current threats in cybersecurity.
Attack Lifecycle	Understand the major factors of an attack including, detection, mitigation, and attribution.
Developer Skills	Be able to understand the importance of software development skills in the security landscape.
Hacker Mindset	Be able to understand the hackers mindset to anticipate what action they will take.

discovery phase (I-1), be “curious” and “motivated to learn” (I-5), and able to make decisions when “you don’t necessarily have all the information that you need” (I-4). Developing patience and curiosity essential for stressful cybersecurity scenarios is necessary to understand how people in different roles think and how to work with them collaboratively.

4.1.4. Holistic Approach.

Six experts stated that cybersecurity professionals need to have a broad understanding of the attack. One explained how cybersecurity professionals need to build a comprehensive vision from various pieces of information (I-1). Another shared that “we need to think about [risk] in multiple dimensions” and that looking at the many primary and secondary effects that an attack could have can provide “a richer and deeper sense of the sophistication of the attack” (I-3). Several interviewees shared examples of unexpected consequences of entire systems collapsing because a seemingly innocuous device goes down. Developing a ”holistic approach” also means understanding the consequences of decisions that are made during the mitigation phase such as “restarting ICS devices,” which can “cause lots of other problems” (I-1). Learning to see the forest from the trees and to think ahead about unintended consequences are key.

4.1.5. Preparation.

Many of the experts (nine) talked about preparation as being essential to mitigating the effect of cyberattacks. Cybersecurity professionals need to be mindful of what proactive measures can be put in place before an attack happens. One expert described this need for preparation as the “linchpin” and emphasized the need to “understand what you’re up against, and then build the defenses against it” (I-7). Other experts mentioned ways to prepare for attacks, including creating a recovery plan for the day after an attack and keeping regular backups (I-2 and I-5), patching vulnerabilities and identifying compensating controls when patches are not possible (I-6), and setting alerts to trigger when abnormal traffic is detected (I-8). Others emphasized the importance of having standard practices in place, such as backups. In the words of I-7, “[What is] the easiest thing we can do for cybersecurity? Backup, right. Yeah. Backup backup backup”.

4.1.6. Cybersecurity Awareness.

Two experts stressed the importance of building cybersecurity awareness into daily lives to mitigate future attacks. It is important to understand the role of security awareness at all levels and be aware of current threats in cybersecurity. One of the experts pointed out that although cybersecurity professionals are generally aware of threats and can identify them, most general workers besides these professionals are not adequately aware of threats (I-7). Another expert emphasized the importance of being mindful of phishing emails, describing the consequences of lack of awareness as “You’re not going to have a hacker break through your firewall or those kinds of old things that used to happen. They just send people emails, and bad things happen after that.” (I-5). For more technical roles, cybersecurity awareness includes a deeper understanding of what constitutes an anomaly. For example, I-6 stated that “You have to know what a baseline of network traffic looks like so that you can recognize an anomaly”.

4.1.7. Attack Lifecycle. Understanding the components of an attack lifecycle such as detection, mitigation, and attribution is an important learning outcome for cybersecurity education (six experts). As per an expert, cybersecurity professionals need to be able to ”identify weaknesses in the system” and ”hunt for issues” (I-1). Another interviewee explained that his “best advice is [to] have a plan that does a risk analysis that looks at the threats. Your vulnerability to the threats helps you understand the consequences of your vulnerabilities to those threats” (I-7). Not only should they know what is wrong, they should understand how attacks show up in their systems and be proactive enough to configure systems to collect data beforehand that could be used later when diagnosing problems (I-1). Experts also acknowledged the problem of teaching attribution due to it being complicated by ”geopolitical elements” such as sophisticated hackers using botnets to reflect attacks from around the world (I-8).

4.1.8. Developer Skills. Another learning outcome that one expert pointed out was the need to understand the importance of software development skills in the security landscape. One expert pointed out that having software development skills provides an upper hand when it comes to securing systems (I-5). Increases in an app-centric ecosystem and cloud deployment are making the network approach of security obsolete. The same expert mentioned, ”It’s all about application security. And you need a developer mindset, who also has the security layer instilled in them. And they’re your secret weapon, you know, in the new world.”

4.1.9. Hacker Mindset. In war, thinking like an opponent is the greatest advantage [42]. This is true in cybersecurity attacks as well. In interview sessions, many experts (six) mentioned the importance of understanding the hacker’s mindset to anticipate what actions they will take (I-1, I-3, I-8). They emphasized the importance of thinking from the offensive side so as to understand hacker actions and motives. One expert mentioned that the purpose of some attacks “isn’t to take someone out, but to cover your tracks while you’re doing something else. (I-8)” Having a hacker mindset is useful to understand these kinds of distractions and focus on the real threats.

4.2. Design Considerations

Experts shared many insights about how to design cybersecurity attack simulations and related educational interventions. Specifically, they offered likely scenarios, roles that participants might play, and other recommendations for building effective simulations. We consider each of these categories in turn.

4.2.1. Scenarios. The most commonly discussed type of cyberattack for a scenario was a ransomware attack as there have been several high-profile cases concerning municipalities in recent years [1, 13]. It was suggested (I-1) that a ransomware attack on a couple of critical infrastructure systems (e.g., power and water) might allow for a strong narrative since it is (a) high impact, (b) unknown who is perpetrating the attack, and (c) an opportunity to go through the entire discovery and incident response process. I-3 also noted that a ransomware attack could introduce the idea of second-order effects and unintended consequences (e.g., a billing system going down leading to power outages). Other common types of attacks mentioned by experts included malware, phishing, and denial of service attacks. When designing training simulations, it is important to address plausible scenarios that people are likely to encounter in real-life. Therefore, designing simulations around one (or more) of these common cyberattacks seems to be a promising approach.

When considering high impact scenarios that would convey the complexity of cyberattacks, many experts (six) talked about attacks on critical infrastructure. One expert (I-7) identified electricity, potable water, and the collection of wastewater as particularly damaging targets: “the cascading impacts of a disruption to those critical services can be really meaningful.” Other experts echoed worries over electrical and water outages, and further expressed concerns over the potential severity of attacks targeting transportation, gas, hospital, or telecommunication systems (I-1, I-6). Additionally, I-7 stated that “You’ve got a lot of small-time operators running critical infrastructures. . . They’re all wearing

Table 3. Expert recommendations for designing cybersecurity simulations.

Recommendation	Description
Consider a variety of factors when planning	Ask questions about the weather, population of affected areas, how long the problem might last, and what kind of long-term impacts could occur when planning a scenario.
Provide opportunities to prepare for an attack	For example, give participants funds to allocate for cybersecurity improvements at the beginning and let those allocations affect the rest of the simulation.
Use a simple risk model	Don't overwhelm participants with the complex algorithms used in professional risk models.
Include experts for consultation	Let participants ask experts about the attacks they encounter. It creates a more realistic work space and teaches participants that security roles cannot be done in isolation.
Add unpredictable elements	Model the unpredictable nature of cyberattacks. Participants should be able to prevent some attacks, but not everything.
Encourage information sharing and collaboration	For example, give each participant access to information that others do not have. Participants must then collaborate and share information in order to see all sides of the problem.
Capture tension between roles and characters	For example, give participants conflicting goals (e.g., forensics wants to find the cause while incident response wants to fix the problem) so they can better understand the interpersonal challenges of teamwork.
Present contradictory information	Help participants disentangle and synthesize information based on their understanding of attribution and make recommendations for action.
Include multiple rounds	Give participants opportunities to demonstrate what they've learned by coming up with solutions across multiple rounds.
Assign a debriefing exercise	Have participants conduct a post analysis on the data and experience, and write a final report to help solidify what they have learned.

four hats in their small organization. So, they're very vulnerable." Experts noted how an attack on one of these critical infrastructures could quickly escalate to affect other systems. Modeling these types of interdependencies and vulnerabilities is key when creating a realistic simulation scenario (I-3).

Experts also felt that it would be important to give participants a scenario where they can experience the different phases of a cybersecurity response (I-1). Ideally, participants might start the simulation in a preparation phase, where they can perform risk assessments, take steps to address vulnerabilities, and create incident response plans (I-2, I-3, I-6, I-7). After this phase, participants would move on to the detection phase where they would quickly determine (hopefully) that an attack had occurred and begin the process of understanding what has happened and the extent of the security breach (I-1, I-8). Next is the response phase where participants would identify steps for dealing with the situation (I1-C1). I-7 discussed the importance of communicating what is happening and what is being done during this phase so that the response team can adequately coordinate their efforts. Another phase mentioned was identifying who was behind the attack, which is often called attribution. I-8 emphasized how this is a complicated issue due to geopolitical elements. The final mitigation phase would occur at the conclusion of the simulation. During this phase, participants would assess and report on their performance during the simulation (I-1) and determine ways to better prepare for the next attack (I-1, I-2, I-5). Moving through these different phases during a simulation would give participants a more realistic experience.

4.2.2. Roles.

The complexity of city and public infrastructure attacks inevitably leads to the involvement of a variety of personnel with different roles. Experts mentioned several possible roles to include in simulations, including a "team lead", an external liaison, an analyst to monitor interface and network "choke points" for "unusual behaviors", and an ICS expert who is “completely focused on machines and equipment” (I-1), as well as incident response and vulnerability analyst roles (I-2). Interviewees stressed the importance of introducing these different roles and how they must coordinate in order to succeed. The importance of sharing information with others was particularly salient. Interviewees (five) gave several examples of cases where people filling different roles needed to share information with one another in order to accurately find, characterize, and in some cases attribute cyberattacks. For example, I-6 mentioned that a person reviewing firewall logs may not have the background to fully understand if some requests are abnormal. They liked the idea of developing simulations wherein people fill different roles and have access to different information that must be shared in order to succeed.

Interviewees (nine) also emphasized some of the tensions that exist based on conflicting incentives that different roles have. For example, I-1 mentioned the conflicts that can occur between information technology (IT) personnel in charge of the computing infrastructure and operations technology (OT) personnel in charge of ICSs. They mentioned how IT and OT personnel do not think in the same way and often OT personnel do not think about security. They recommended building a simulation that could bring this tension to the forefront by having fictional IT & OT characters at an organization that was attacked not get along or have some misunderstanding. Another issue interviewees raised was the tension between incident responders who are trying to immediately stop things from causing damage and forensic experts interested in capturing data to identify how people got in and who is behind it.

Interviewees (four) also emphasized how common it is for multiple institutions to get involved after a significant attack. I-6 recommended that simulation designers: “Do something big that includes different agencies. Then you’ll have a real scenario.” These include different local agencies (e.g., utility companies, city and county government institutions), state and federal agencies (e.g., DHS, FBI, CERT experts) who often support local staff with less experience after significant attacks, and formal and informal professional cybersecurity networks. Modeling the sociotechnical side, and not just the technical issues, was particularly important to many of our interviewees. For example, I-8 mentioned the need to consult with other cybersecurity experts, not just documentation: “I cannot stress enough that the community is a big deal. So I’m on a few mailing lists where I’ll see people, hey, I’m seeing this type of traffic. Has anyone else seen this? And then some will say, yeah, we started seeing this Tuesday at 5am and a no. So yeah, sometimes you don’t know what to get out of isolation [until you] taste things together. And you hear from other operators and what they’re seeing across the internet.”

4.2.3. Simulation Recommendations. Many of the experts had either designed cybersecurity simulations or participated in simulations and they offered several specific recommendations (not already covered) for making them more realistic and effective. These recommendations are summarized in Table 3.

5. Discussion

As cyberattacks on city and public infrastructure become increasingly common and harmful, it is critical that we train the professional workforce to prepare and respond appropriately. This is a challenging task, given the complexity of such attacks that often include multiple institutions at the local, state, and federal level; different technical and non-technical roles; and a variety of different information technologies and ICSs. Based on 8 interviews of 12 diverse cybersecurity experts, many of whom have dealt directly with city and public infrastructure attacks, we have identified learning outcomes and suggestions for those designing simulations and other experiential learning interventions.

Over the past year, our research team has been designing and building a PCS [38, 39] called MIRROR (Municipal Incident Response and Risk Operations Range) focused on a cyber-physical attack on a fictional city and its public infrastructure. Of necessity, we have only been able to take on a handful of the key learning outcomes and design considerations outlined in this paper. The insights provided by our expert interviews have inspired our focus on a role-based, collaborative simulation that introduces several key aspects of the attack lifecycle within the context of a realistic ransomware and malware scenario. Below is a brief discussion of how the information in this paper has helped us design the MIRROR playable case study.

Teams of learners will join together into groups of 4 members, each of whom will take on the role of a system administrator, SCADA technician, security operations center analyst, or a communications manager. They will interact with fictional characters, such as the CISO of Bronze Falls (the fictional city) and content experts who provide educational scaffolding and tasks. The goal is to introduce them to the entire attack lifecycle, including three major phases of planning, incident response, and attribution, each of which includes a collaborative activity. For example, in the “planning” phase, the team must collaboratively decide what security controls to invest in. To help make these decisions, each player is given information specific to their role and advice from a fictional supervisor in their own organizational unit about what controls are important. They are also introduced to risk assessment calculations and given a "breach report" with data on prior attacks on city and public infrastructures. Because they each receive role-specific, potentially conflicting information, the importance of information brokering is underscored, as is an understanding that different information is available to people in different roles.

During the "incident response phase" players must respond to a ransomware attack that is spreading through the city's IT department devices, as well as a malware attack affecting SCADA devices. Again, each role has conflicting information and different actions they can take, requiring team members to effectively share information and coordinate actions to mitigate the unfolding attack. For example, the SCADA technician can see data about SCADA devices and choose to investigate or turn off a device, while the communications manager sees citizen complaints about the impact of the attack and can choose to notify the public about a problem. The team's effectiveness is determined by both first-order effects on the devices that are damaged or shut off and second-order effects on city residents as a result of the attack [43]. The "attribution" phase requires players to synthesize and reconcile evidence to determine the source of the cyberattack. Like the previous collaborative decision-making tasks, this activity includes similar role-specific information that can contradict other role's information, suggesting the inherent uncertainty of initial attribution attempts.

These design elements emphasize many of the learning outcomes, scenarios, and design ideas identified in this paper. We aimed to provide a holistic, highly contextualized view of a complex, real-world scenario with different roles and the need to effectively broker information through the entire attack lifecycle. We have also embedded many suggestions such as using a simple risk model, including a debriefing exercise, presenting contradictory information (e.g., in the attribution phase), including experts for consultation, etc. Of course, our take on the simulation is just one of many - focused largely on those new to cybersecurity. We are excited to see what other educational designers develop from the many useful ideas expressed by the experts whose ideas we have synthesized in this paper.

Although systematically analyzed, our study is not without limitations. It represents the opinions of 12 individuals, during 8 interview sessions. Fortunately, it includes interviewees from a range of backgrounds, who were well aware of attacks on city and public infrastructures. However, we do note that one third of the participants were from the academic community and not practitioners, which could be seen as a limitation. Additional interviews, including ones with people filling different cybersecurity professional roles would likely lead to additional insights. We chose to use a thematic analysis approach that let the themes emerge from the data. While we believe this was useful in staying true to the voice of the experts, it does not connect as directly to existing cybersecurity frameworks (e.g., NIST Framework) as it would have if we had coded the data into an existing framework. Future work could expand on this paper by increasing the number and diversity of interviewees or applying alternative coding strategies. Our hope is that the learning outcomes and design ideas shared in this paper will inspire new educational experiences to help improve the security of our city and public infrastructures.

6. Acknowledgements

Research funded by the National Science Foundation (NSF) grants 1915563 and 1915620.

References

[1] C. Fisher, "A ransomware attack is holding Baltimore's networks hostage," May 2019. www.engadget.com.

[2] T. Douglas, "What Can We Learn from Atlanta?," 2018. www.govtech.com.

[3] A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, 2019.

[4] D. F. Norris, L. Mateczun, A. Joshi, and T. Finin, "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity," *Public Administration Review*, vol. 79, no. 6, pp. 895–904, 2019.

[5] A. Conklin and G. B. White, "e-government and cyber security: The role of cyber security exercises," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, vol. 4, pp. 79b–79b, 2006.

[6] N. Allen, "Cybersecurity weaknesses threaten to make smart cities morecostly and dangerous than their analog predecessors," *USApp–American Politics and Policy Blog*, 2016. Publisher: The London School of Economics and Political Science.

[7] D. Walcroft, "Smart cities: five smart steps to cybersecurity." www.pwc.com.

[8] G. B. White, "The community cyber security maturity model," in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 173–178, 2011.

[9] J. Hammerstein and C. May, "The CERT approach to cybersecurity workforce development," tech. rep., Carnegie Mellon University Pittsburg PA Software Engineering Institute, 2010.

[10] K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," *Wired Magazine*, vol. 3, 2016.

[11] T. Chuang, "How SamSam ransomware took down CDOT and how the state fought back – twice," Feb. 2020. coloradosun.com Section: _Homepage.

[12] K. Yedakula, "Here's what went wrong in Baltimore ransomware attack that cost the city over $18.2 million | Cyware Hacker News," Oct. 2019. cyware.com.

[13] N. Popper, "Ransomware Attacks Grow, Crippling Cities and Businesses - The New York Times," Feb. 2020.

[14] I. Homel and S. Staff, "Teen Hacker in Poland Plays Trains and Derails City Tram System," Feb. 2008. inhomelandsecurity.com Section: Cybersecurity.

[15] BBC News, "Hack attack causes 'massive damage' at steel works - BBC News," Dec. 2014.

[16] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016. Publisher: IEEE.

[17] W. Crumpler and J. A. Lewis, *Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS), 2019.

[18] H. Al-Mohannadi, I. Awan, J. Al Hamar, Y. Al Hamar, M. Shah, and A. Musa, "Understanding awareness of cyber security threat among it employees," in *2018 6th International Conference on Future Internet of Things and Cloud Workshops*, pp. 188–192, IEEE, 2018.

[19] M. Malatji, S. Von Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Information & Computer Security*, 2019. Publisher: Emerald Publishing Limited.

[20] E. Walker, D. Witkowski, S. Benczik, and P. Jarrin, "Cybersecurity – the Human Factor," 2017.

[21] P. W. Coopers, "The Global State of Information Security Survey 2018," *Price Waterhouse Coopers*, 2014.

[22] P. R. Clearinghouse, *A chronology of data breaches*. 2020.

[23] G. Conti, T. Cross, and D. Raymond, "Pen Testing a City," *Black Hat USA*, 2015.

[24] L. J. Thomas, M. Balders, Z. Countney, C. Zhong, J. Yao, and C. Xu, "Cybersecurity Education: From Beginners to Advanced Players in Cybersecurity Competitions," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 149–151, 2019.

[25] H. Kavak, J. Padilla, D. Vernon-Bido, R. Gore, and S. Diallo, "A Characterization of Cybersecurity Simulation Scenarios," 2016.

[26] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, and D. Weintrop, "Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games," *Simulation & Gaming*, 2020.

[27] A. Brilingaitė, L. Bukauskas, V. Krinickij, and E. Kutka, "Environment for cybersecurity tabletop exercises," in *ECGBL 2017 11th European Conference on Game-Based Learning*, pp. 47–55, Academic Conferences and publishing limited, 2017.

[28] J. Giboney, D. Hansen, J. Mcdonald, B. Jonathan, J. Tanner, D. Winters, and E. Bonsignore, "Theory of Experiential Career Exploration Technology (TECET): Increasing cybersecurity career interest through playable case studies," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[29] M. E. Gredler, "Games and simulations and their relationships to learning," *Handbook of research on educational communications and technology*, vol. 2, pp. 571–581, 2004. Publisher: Mahwah, NJ: Lawrence Erlbaum Associates Publishers.

[30] Cognition and T. Group, "Anchored instruction and situated cognition revisited," *Educational Technology*, pp. 52–70, 1993. Publisher: JSTOR.

[31] S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi, "The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game," *IEEE Transactions on Software Engineering*, vol. 45, no. 5, pp. 521–536, 2019.

[32] I. Graffer, M. B. Line, and K. Bernsmed, "Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations," *NISK Journal*, pp. 58–69, 2015.

[33] J. Esquibel and E. Mitchell, "Jack Voltaic 2.0: Threats to Critical Infrastructure," 2019.

[34] D. Noyes, "Cyber Security Testing and Training Programs for Industrial Control Systems," Tech. Rep. INL/CON-12-24615, Idaho National Laboratory, 2012.

[35] H. Holm, M. Karresand, A. Vidström, and E. Westring, "A survey of industrial control system testbeds," in *Nordic Conference on Secure IT Systems*, pp. 11–26, Springer, 2015.

[36] S. Panzieri, R. Setola, and G. Ulivi, "An agent based simulator for critical interdependent infrastructures," in *Securing Critical Infrastructures, CRIS2004: Conference on Critical Infrastructures*, pp. 25–27, Citeseer, 2004.

[37] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, "Critical infrastructure interdependency modeling: a survey of US and international research," *Idaho National Laboratory*, vol. 25, p. 27, 2006.

[38] J. Balzotti and D. Hansen, "Playable case studies: A new educational genre for technical writing instruction," *Technical Communication Quarterly*, vol. 28, no. 4, pp. 407–421, 2019. Publisher: Taylor & Francis.

[39] J. Mcdonald, D. Hansen, J. Balzotti, J. Tanner, D. Winters, J. Giboney, and E. Bonsignore, "Designing Authentic Cybersecurity Learning Experiences: Lessons from the Cybermatics Playable Case Study," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[40] J. Lazar, J. H. Feng, and H. Hochheiser, *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[41] V. Braun and V. Clarke, "Thematic analysis.," in *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological.*, APA handbooks in psychology®., pp. 57–71, Washington, DC, US: American Psychological Association, 2012.

[42] S. Tzu, *The Art of War*. Place of publication not identified: Filiquarian Pub., 2006. OCLC: 764419687.

[43] Charles T. Harry and Nancy W. Gallagher, "An Effects-Centric Approach to Assessing Cybersecurity Risk," tech. rep., Center for International and Security Studies at Maryland, University of Maryland College Park, Mar. 2019.