Communications of the Association for Information Systems

Volume 46 Article 8

2-2020

Responding to Cybersecurity Challenges: Securing Vulnerable U.S. Emergency Alert Systems

Andrew W. Green
Kennesaw State University, agreen57@kennesaw.edu

Amy B. Woszczynski
Kennesaw State University

Kelly Dodson
Kennesaw State University

Peter Easton
Kennesaw State University

Recommended Citation

Green, A. W., Woszczynski, A. B., Dodson, K., & Easton, P. (2020). Responding to Cybersecurity Challenges: Securing Vulnerable U.S. Emergency Alert Systems. Communications of the Association for Information Systems, 46, pp-pp. https://doi.org/10.17705/1CAIS.04608

Communications of the Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04608 ISSN: 1529-3181

Responding to Cybersecurity Challenges: Securing Vulnerable U.S. Emergency Alert Systems

Andrew Green
Michael J. Coles College of Business
Kennesaw State University
agreen57@kennesaw.edu

Amy B. Woszczynski
Michael J. Coles College of Business
Kennesaw State University

Kelly Dodson
Michael J. Coles College of Business
Kennesaw State University

Peter Easton
Michael J. Coles College of Business
Kennesaw State University

Abstract:

Emergency alert systems (EASs) in the United States (US) form part of the nation's critical infrastructure. These systems rely on aging platforms and suffer from a fragmented interconnected network of partnerships. Some EASs have an easily identifiable vulnerability: one can access their management website via the Internet. Authorities must secure these systems quickly. Other concerns also exist, such as the lack of policies for reporting vulnerabilities. To begin to assess EASs in the US, we used Shodan to evaluate the availability of these websites in six southeastern states. We found 18 such websites that one could access via the Internet and that required only requiring user credentials to login into. Next, we searched for published policies on reporting vulnerabilities; we found no vulnerability-disclosure policies for any system we identified. To identify, prioritize, and address EAS vulnerabilities, we present a list of technical and management strategies to reduce cybersecurity threats. We recommend integrated policies and procedures at all levels of the public-private-government partnerships and system resilience as lines of defense against cybersecurity threats. By implementing these strategies, EASs in the US will be positioned to update critical infrastructure, notify groups of emergencies, and ensure the distribution of valid and reliable information to at-risk populations.

Keywords: Emergency Alert System, Vulnerabilities, Critical Infrastructure, Cybersecurity Policy, Cybersecurity Research, Emergency Preparedness, Vulnerability-disclosure Policies.

This manuscript underwent peer review. It was received 11/19/2018 and was with the authors for 3 months for 1 revision. Kent Marett served as Associate Editor.

1 Introduction

In 2013, individuals in Michigan, Montana, and New Mexico found themselves in the middle of the zombie apocalypse when numerous emergency alert systems (EASs) improperly sent the following alert (Roberts, 2013; Reuters, 2013; Storm, 2013):

> *Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living. Follow the messages on screen that will be updated as information becomes available. Do not attempt to approach or apprehend these bodies as they are considered extremely dangerous.*

In reality, cybercriminals had managed to access these systems and send the messages. However, the EAS owners had made it easy: they still used default passwords that they had not changed since they received the hardware. Further, individuals could publicly access the initial passwords on the Internet along with other operating instructions from Digital Alert Systems/Monroe Electronics (DAS/ME), a leading hardware provider for the EAS network. DAS/ME specifically advised all users to change the default passwords immediately; however, many EAS owners ignored the password guidance to their peril. While we cannot prevent an emergency, we can reduce EAS vulnerabilities and decrease the likelihood that cybercriminals will access EAS without authorization. Reducing vulnerabilities increases confidence in the alerts sent to the population as a whole. Zombie apocalypse announcements, in contrast, cause people to doubt the integrity of the messages received and to question the underlying reliability of EASs as a whole.

The available evidence tends to show that U.S. EASs, as part of the nation's critical infrastructure, lack sufficient protection (Lanier, 2018). While many would assume that vulnerabilities found in EASs have decreased since the widely publicized zombie apocalypse hoax in 2013, the evidence available fails to support that assumption. Mike Davis, who discovered the original zombie apocalypse vulnerability, found that more EASs still used default passwords months after his original alert to vendors (Ollmann, 2013).

More recently, Hawaii's EAS experienced a public and embarrassing incident due to human error when someone pressed the wrong button (Kang, 2018). The SMS message, which all Hawaii residents received, read: "BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL" (Faris, 2018). It took 38 minutes to alert the public that the message was a false alarm (Sidner & Andone, 2018). False messages about incoming missiles do not inspire public confidence any more than hoaxes about the zombie apocalypse. However, the more pressing concern here concerns the fact that outsiders can take control of these systems and send (or not send) whatever messages they chose.

EASs should securely distribute valid and reliable information to the relevant population in an effective and timely manner. Past performance does not lead to confidence in EASs in the US. In this paper, we propose that EAS owners use technical guidelines and management strategies to plan and prepare for vulnerabilities in fragmented, decentralized EASs. Sadly, some EAS owners do not follow technical guidelines or use management strategies to secure their networks, which increases opportunities for cybercriminals to compromise systems. The problem also involves insufficient funding for national, regional, state, city, county, and other government bodies; without funding, the EASs remain vulnerable to critical failures that may have a catastrophic and cascading impact on the general public. System resilience in the face of constant cybersecurity challenges provides an essential method to overcome inevitable failures, but insufficient funding limits opportunities to protect EASs.

Previous academic work has not evaluated the security of the EASs or countermeasures that EAS owners or manufacturers could take to secure and protect this critical U.S. infrastructure system. With previous instances of demonstrated insecurity, we believe that this study is timely, relevant, and critical. To determine the cybersecurity challenges facing EASs, we took a two-step approach and analyzed EASs in light of: 1) the number of Internet-accessible EAS management websites in the Southeastern United States accessible via the World Wide Web (WWW) and 2) the publicly available guidelines about reporting vulnerabilities. We provide technical guidelines and managerial recommendations that encourage cybersecurity researchers and organizations to harmoniously work together to identify and resolve vulnerabilities present in U.S. EASs.

This paper proceeds as follows: in Section 2, we examine the current state of the EASs in the US. In Section 3, we outline steps that the EAS network may take to reduce vulnerabilities. In Section 4, we discuss the method we followed to collect data about EASs in the Southeast United States. In Section 5,

we report our results, which we analyze in Section 6. In Section 7, we discuss the study's limitations and possibilities for future research. Finally, in Section 8, we conclude the paper.

2 Current State of the U.S. Emergency Alert Systems

2.1 EAS overview

In the US, the EAS is a national public warning system that individual television, radio, cable, and satellite broadcasters use to deliver emergency alerts to the public (Federal Communications Commission, 2018). The EAS primarily allows affected people to receive critical, timely, and relevant information regarding an emergency. At the national level, the U.S. President may call for an announcement to the public regarding a national emergency; more commonly, state and local authorities use the EAS's decentralized architecture to distribute emergency messages on a statewide or local level (Federal Communications Commission, 2018).

EAS authorities can send messages via two different methods. In the first method, they format an EAS message using the proper protocol and transmit it via a daisy-chain style distribution method from broadcaster to broadcaster until they have fully distributed the message (Federal Communications Commission, 2018). In the second method, they send EAS messages via the Internet through the Integrated Public Alert and Warning System (IPAWS), a system that the Federal Emergency Management Agency (FEMA) administers (Federal Communications Commission, 2018). In this study, we examine vulnerabilities present in decentralized EASs at the individual broadcaster level, not in the IPAWS.

2.2 Definitions

In this paper, we use the following terms:

- Emergency alert system (EAS): a public warning system that requires broadcasters to provide communications capabilities to the U.S. President and state and local authorities to address the affected population during an emergency (Federal Communications Commission, n.d.).
- Internet-facing EAS management website: a website that provides administrative access to an individual broadcaster's EAS infrastructure. Individuals can access this website via the Internet with nothing other than a Web browser; users authenticate with a username and password. Authorized users can exercise full control over the individual broadcaster's EAS infrastructure from this website; this control includes the ability to send EAS messages, disable the EAS entirely, erase files, add files, and similar administrative-level privileges once a user authenticates.
- Broadcasters: any local, regional, or state system that provides publicly accessible radio or television transmissions or telecommunications services (landline and cellular telephone).
- EAS supply chain: the network of stakeholders involved in receiving EAS signals, translating and verifying received signals, and sending emergency alerts to broadcasters and other stakeholders (e.g., people in an affected region). For EASs, the supply chain includes EAS manufacturers (such as Digital Alert Systems/Monroe Electronics, Everbridge, Inspiron Logistics, and Vesta Public Safety/Cassidian Communications); EAS managers at the local, state, and regional levels; and the population receiving the emergency warning alerts.

2.3 History of EAS Vulnerabilities

As Table 1 shows, EAS vulnerabilities have existed for some time. In the 1990s and 2000s, individuals began to distribute information on a wide-scale over the Internet. Access became ubiquitous, and graphical user interfaces allowed users to easily, quickly, and efficiently access information. Curious people chanced on vulnerable systems, while malicious actors began to capitalize on system vulnerabilities. Once individuals identified vulnerable systems, they began sharing information with a widely dispersed and Internet-connected population.

Meanwhile, Michigan, Montana, and New Mexico received devastating news in 2013: the zombie apocalypse had begun (Storm, 2013). In that case, local, state, and federal authorities did not change the default passwords for their systems; since Monroe Electronics published their manual online (which included the default credentials), cybercriminals had easy access and could log into the system with

details found there. In addition to the default credentials being available on the Internet, individuals could access the EAS management websites via the Internet (Reuters, 2013). Several months after the zombie hoax, the number of vulnerable systems increased (Roberts, 2013), despite the embarrassing zombie apocalypse message.

Table 1. Recent EAS/EAN Incidents

Year	Location	Description	Outcome
2007	Illinois	False EAN message sent	An operator left satellite receiver on by mistake
2011	Nationwide	FEMA and FCC conduct the first live test of EAN	18% failure rate
2013	Michigan, Montana, New Mexico	TV stations broadcast false "zombie apocalypse" warning	Default passwords not changed
2014	Texas, Georgia, Michigan	TV stations broadcast false EAN message	Message sent in error by nationally syndicated radio show
2016	Utica, New York	TV station broadcasts false hazardous materials incident warning	A decoder at WKTV improperly sent alert; no further details
2016	Nationwide	First successful test of the EAN completed, using audio and video	Less than 44 percent of television tests included the slide, text crawl and audio components that were required to reach persons with disabilities
2017	Dallas, TX	City alert sirens triggered	Operated on radio frequencies and may not have been encrypted
2018	Nationwide	The first test of the EAN on mobile phones completed	Most users received the test message; few details available
2018	Hawaii	False incoming ballistic missile alert message sent	Message sent in error by state employee; no explanation given for 38 minutes since Governor forget Twitter password

More recently, on 28 September, 2016, cybercriminals compromised the EAS at WKTV, a TV station in Utica, New York, and broadcasted a false alarm about a hazardous material incident (WKTV, 2016). In Facebook posts, WKTV initially blamed FEMA for sending an error code, but then determined it was an error in their decoder (https://offgridsurvival.com/femas-emergency-alert-system-hacked-warns-hazardous-materials-disaster/). Shortly thereafter, on 7 April, 2017, Dallas residents awoke to sirens in the middle of the night; authorities could not deactivate the sirens for 90 minutes (Hub, 2017). In the Dallas case, cybercriminals accessed the system using radio frequencies, and the system may not have been encrypted, which would have made it more vulnerable to threats (McFarlane, 2017). Almost a year later, in early 2018, Hawaii made news when it warned residents that a missile was inbound and that residents should take cover immediately (Sidner & Andone, 2018). After the Hawaii incident, experts again called for federal, state, and local officials to work together to identify and resolve vulnerable systems to ensure they could immediately issue corrections to false alerts (Kang, 2018). While the Hawaii debacle worried some EAS providers, Demer (2018) argued that other states were unlikely to experience an attack similar to Hawaii due to additional built-in checks that made them less vulnerable than Hawaii; checks included using ready-made alerts and requiring at least two employees to sign off on a real alert.

Cybercriminals have not limited their attacks to the local or state levels. For instance, on 26 June, 2007, Illinois state officials distributed an Emergency Action Notification (EAN), a direct message from the President of the United States (FEMA, 2007). In the 2007 incident, a local contractor accidentally left a satellite distribution receiver in the “on” mode, and the system sent the message to the designated area. FEMA promised to better coordinate with the FCC and local, state, and federal authorities when conducting tests in the future. We concur with their call for more coordination throughout the EAS network.

In 2011, the FCC and FEMA did a live test for an EAN, and about 18 percent of systems failed to receive the message (Fletcher, 2016b). The next test for the EAN system did not take place until 2016.

Then, in October 2014, cable subscribers in Austin, Atlanta, and Detroit received a false EAN; the message told AT&T U-verse viewers that they could not change the channel and to wait for an upcoming message from the White House regarding a national emergency (Pallotta, 2014). A blog post by user

ATTU-verseCare (https://forums.att.com/t5/Watching-U-verse-TV/An-emergency-notification-with-no-emergency/td-p/4134018/page/7) indicated the problem arose due to a message sent in error by a nationally syndicated radio show unaffiliated with AT&T.

Two years later, on September 28, 2016, the nation conducted the first successful test of the EAN, this time using audio and video (Fletcher, 2016a). However, while the test results improved from 2011, Wireless RERC (2016) noted that less than 44 percent of television tests included the slide, text crawl, and audio components that a fully successful test required; further, they noted several issues that the nation needed to address to improve access to those with disabilities and to those who speak languages other than English. States responded to these deficiencies by offering sign-up sheets for persons with disabilities. However, they could still not reach the targeted group with over 80 percent of counties reporting accessibility violations (Wentz et al., 2014).

More recently, in October, 2018, government authorities tested the EAN on mobile phones for the first time. While most users received the message, some did not; they may have been out of range of a cell phone tower, had their phone turned off or in airplane mode, had a cell phone that interacted with the broadcast message in unexpected ways, or other unanticipated errors (Dreyfuss, 2018). We could not find if those with disabilities, such as individuals with vision and hearing impairments, received the alerts in the format needed. Learning about the errors with a nationwide text alert may allow the EAS network to strengthen its ability to reach the population in a real national emergency; however, since local and/or state authorities issue most alerts, a focus on vulnerability at the national level cannot sufficiently ensure EASs' capabilities.

2.4 System Vulnerability

In order for EASs to remain relevant and trustworthy to the population, authorities must minimize the number of false alerts broadcast. Dispensing reliable data every single time ensures that people recognize the information's validity, relevance, and timeliness. With too many inaccurate alerts, the public will likely begin to question the information provided even during an actual emergency. As a part of the nation's critical infrastructure, many may assume that our government tests for and protects against inaccurate data with significant cybersecurity safeguards in place to ensure protection from threats. However, cybercriminals could have a "field day" with emergency alert systems due to their vulnerability (Albanesius, 2013). Dodril (2016) argues that EASs are as vulnerable to attack as other national infrastructures and warns about the potential impact if cybercriminals compromise EASs. John Hickenlooper, Governor of Colorado, has voiced concerns about the security of EASs in saying that "the next battlefront is likely not a field or town, but a computer network that supports our critical infrastructure" (Matthews, 2014). With U.S. infrastructure continuing to deteriorate over time (Hemme, 2015) and with authorities using old technology and programs initially developed in the 1980s (McFarlane, 2017), EASs are clearly vulnerable to cybercriminals (Constantin, 2013). Even when EASs do not connect directly to the Internet with open access, authorities have to worry about vulnerabilities in the equipment that they use to transmit the alerts (Albanesius, 2013). In some cases, EASs remain vulnerable due to insufficient preparation and awareness about cybersecurity issues that exist (Hub, 2017). One cannot easily resolve the problem.

While the recent cyberattacks on EASs demonstrated how attackers used vulnerabilities with little community impact, a much more severe scenario involves a domestic or foreign terrorist attack on the EAS. Cyberterrorists could compromise the EAS as part of a broader attack on a population; for instance, they could send a false message directing citizens to move to a designated staging area and then attack the citizens staging there. Similarly, they could broadcast road closings using the EAS and direct residents to a particular route, which they could then attack. While these cyberterrorist attacks have not yet occurred, the EAS's vulnerability remains a serious concern particularly given that local or private organizations own 85 percent of critical infrastructure (Egli, 2013); thus, the EAS requires protection at the local, most decentralized level the most. With cybercriminals working together (sometimes at the direction of nations in opposition to the US), state and local EASs may find it quite challenging to mount a sustained defense (Claus, Gandhi, Rawnsley, & Crowe, 2015). At the local level where organizations receive less funding and have less cybersecurity expertise, the risk is even more significant than at the national level (McFarlane, 2017).

Further complicating efforts to protect the EASs, organizations often view disaster management in a silo manner in which they consider each level in the chain without planning for the interconnected network (Egli, 2013). Without coordination throughout all EAS levels, local levels will likely continue to experience

vulnerable EASs. Involvement at the federal level may be needed to combat these threats. For example, if federal regulations specify minimum cybersecurity protections and controls, then EAS managers at all levels must invest more money into securing their systems to reduce system vulnerability (Li, 2015).

Contemporary technology developments emphasize the importance of each link in the system no matter how small or large. Each link in the partnership must be prepared to address continued cybersecurity challenges. For instance, the rise of the Internet of things (IoT) has dramatically increased the number of connections that individuals, private organizations, and the government must secure. These connections, along with the need for remote access to critical systems, increase EASs' vulnerability to unauthorized access (McFarlane, 2017; Meshkati & Tabibzadeh, 2016). While authors cannot easily secure all connections throughout the EAS supply chain (Morrison, 2013), they must implement cybersecurity controls, policies, and processes to address the vulnerabilities present in the vast network of interconnected national, state, regional, and local EASs. If cybercriminals find it easier to attack local or state-level EASs, then they will focus their efforts accordingly; each connection presents a potential system-wide vulnerability—a definite argument against a silo approach to securing vulnerable systems.

To reduce vulnerabilities in EAS, organizations need to have a trained and aware staff and need to emphasize security education, training, and awareness (SETA) policies at all levels. However, local governments continue to face underfunded SETA opportunities. Meshkati and Tabibzadeh (2016) found that EAS authorities often believe that their personnel lack adequate training in security and information protections; in fact, just over 70 percent of local governments have reported that insufficient end-user training represented a modest or severe barrier to cybersecurity efforts. Without sufficiently training those who use systems, cybersecurity protections may be less effective. Moreover, as long as cybercriminals continue to believe that local systems remain vulnerable and that they likely will not be caught, they will continue to search for and penetrate these access points (Metivier, 2017). The ongoing struggle to hire qualified, well-trained cybersecurity experts to work with the EASs at substantially lower government wages compared to their peers in the private sector compounds the system-vulnerability issue (Nixon, 2016). Attacks on points in the EAS's critical infrastructure continue unabated, which highlights the need for a clear, unambiguous, coordinated method to secure vulnerable systems throughout the EAS network.

3 Steps to Reduce Vulnerabilities

Given that current cybersecurity policies and practices remain fragmented and non-cumulative across all the partners in the critical infrastructure supply chain, we require an overarching, integrated risk-management approach (DiMase, Collier, & Linkov, 2015). Partners in the EAS supply chain have diverse backgrounds that complicate efforts to work together, and cybersecurity professionals face social dynamics that they may not know how to manage. An EAS network may include weather and disaster forecasters who have a strong science background, media professionals who have a more liberal arts education, and the public with diverse backgrounds. The difficulty in communicating with these diverse partners becomes even more complicated when technology partners enter the picture. This diversity in backgrounds and experience hampers communication and offers numerous challenges for planning and implementing cybersecurity (Morss, Demuth, Bostrom, Lazo, & Lazrus, 2015). While this diverse network complicates efforts to implement risk-management plans, it does allow the opportunity to build on local and traditional knowledge and strategies to better understand the complex EAS network (Baudoin, Henly-Shepard, Fernando, Sitati, & Zommers, 2016). All entities no matter their backgrounds need to more closely coordinate to properly manage cybersecurity (Borchert, 2015). Further, such entities must develop and implement technical shutdown procedures as part of an overall risk-management plan and ensure they can use a backup system if needed to provide valid, reliable, accurate, and timely data and information during an emergency (Hub, 2017; Wirth, 2017). Thus, cybersecurity professionals face the challenge of understanding the social dynamics in the organization, deploying management practices in response, and then developing technical controls to reduce vulnerabilities.

Cybersecurity professionals developing risk-management plans for EAS authorities should clearly understand infrastructure dependencies, such as the public-private-government partnerships in most EASs, and should be able to determine the cascading damages that may result from attacks (Zeichner, 2001). They also require technical expertise in the field to understand the impact that cyberattacks may have. Cybersecurity risk-management plans focus on minimizing risk, particularly at the national level, which means they face heavy regulation. In contrast, cities, counties, and localities face fewer regulatory requirements (McFarlane, 2017), which opens the door to potential vulnerabilities. When regulators set minimum risk-management requirements for states, cities, and counties, however, the EAS supply chain

members complain that the requirements become burdensome and expensive. In September, 2018, the Federal Communications Commission (FCC) established the Alert Reporting System (ARS), which allows states to electronically file their EAS plans (Federal Communications Commission, 2018). The FCC took this step to ease the reporting requirements and associated administrative burdens for state-level emergency communications committees while still maintaining minimum risk-management levels.

While some partners focus only on the local level and, thus, exclude partners at other levels (Egli, 2013), risk-management policies should consider all partners in the public-private-government chain, the actors that distribute and receive information, such as the public at large, forecasters, media liaisons, and so on. Deeply understanding the partners can help EAS authorities recognize relevant social structures and how to integrate management and technical best practices into efforts to design, develop, and maintain the EAS supply chain. Further, companies should consider acquiring cybersecurity insurance in addition to typical business insurance to protect against attacks; standard insurance likely will not cover digital assets (Hub, 2017). Risk management does not eliminate risks but develops an overall plan to reduce the amount of damage done when a risk materializes. When a cybersecurity breach inevitably occurs, a good risk-management plan will help ensure that the network remains resilient (Jung & Song, 2015) and can respond to the threat. Cybersecurity professionals must work with EAS authorities to develop a risk-management plan while educating those in the network about how to minimize threats to the EAS supply chain.

Throughout this section, we discuss the complexities in responding to cybersecurity challenges. Cybersecurity professionals must not rely on technical expertise alone. Instead, they must keenly recognize social dynamics and how people will use systems in unintended ways and, thus, develop managerial policies that account for social dynamics. Having technical skills without understanding social skills (or vice versa) will not lead to ideal outcomes. In Section 3, we examine steps to reduce vulnerabilities. In particular, we divide these vulnerabilities into predominantly technical issues or predominantly social issues, though we acknowledge the two often overlap. We begin with technical cybersecurity issues, which include prioritizing threats, using appropriate encryption, and testing systems.

3.1 Technical Issues

3.1.1 Prioritizing Threats

All threats differ. Some threats, though unlikely to occur, could present devastating and cascading effects on EASs. Other threats, while likely, may present less potential damage if one exploited the vulnerability. Cybersecurity professionals must prioritize threats and provide protections in line with the likelihood a threat will occur and its severity. Borchert (2015) asserts that organizations should prioritize and manage “core issues” (serious, short term technical threats) and “cross-cutting issues” (long-term threats, such as aging infrastructure). EAS authorities must evaluate vulnerable systems at all levels for their impact on the system as a whole. They should address those threats that may interfere with EASs’ ability to deliver information to the right people at the right time and in the right format first as a core issue and then proceed to less important ones. Aging infrastructure that, over the long term, may affect how all systems on the interconnected network perform represents a cross-cutting issue; thus, EAS authorities should address this issue in long-term planning. Cybersecurity professionals should stay abreast of current developments that may present a threat to EASs, such as using social media to identify, prioritize, and respond to threats (Sheffi, 2015). EAS authorities should periodically re-evaluate threats, however, since long-term threats may become a core issue if they do not address them promptly.

3.1.2 Using Encryption

Researchers widely agree that EAS messages require encryption (Loukas, Gan, & Tuan, 2013; Seddigh, Nandy, & Lambadaris, 2006; Shu, Lee, & Yannakakis, 2006). In the Dallas siren example that we discuss in Section 2.3, cybercriminals accessed the system through unencrypted radio signals (Hub, 2017); strong encryption may have prevented that cyberattack from taking place. Populations that receive EAS messages are transient and change often and sometimes in unexpected manners. From a public policy and safety perspective, when an emergency happens, citizens do not differ from people who are visiting or passing through an area—everyone in the affected region needs to receive EAS messages about emergencies. Schulzrinne and Arabshian (2002) have proposed a method to allow user devices to auto-subscribe to alerts based on their geographical proximity. However, they did not mention message

encryption in this method. Thus, sending an EAS message (encrypted or not) to an unidentified and fluid population subset is a non-trivial matter.

Assuming we find a way to identify the changing population in a specific geographical location, we must contend with technology limitations. In response to this problem, Fiat and Naor (1993) investigated whether it was possible for two devices that previously did not know each other to establish an encryption key to allow the sender to securely transmit data to the receiver; they introduced the concept of broadcast encryption to send encrypted messages from a centralized broadcast source to authorized recipients. Broadcast encryption gained support from the community (Lotspiech, Nusser, & Pestoni, 2002) and spawned various related schemes such as the layered subset difference broadcast encryption scheme (Halevy & Shamir, 2002) and the identity-based broadcast encryption scheme with personalized messages (Xu, Liao, Qiao, Liu, & Yang, 2015).

On the surface, broadcast encryption seems like the perfect solution to address issues with verified and trust sources sending secure messages. However, the underlying requirements for the scheme to work, such as smart cards or pre-distributed encryption keys, make the system impractical for delivering EAS messages. As Shu et al. (2006) have noted, broadcast encryption works well in pay television programming and Internet-based software distribution but poses implementation challenges in EASs.

Thus, we can see that encryption in EAS message dissemination involves much complexity and a wide array of concerns and obvious technology limitations. Possible solutions to address these concerns fall outside our scope here and even outside the scope of current practical technology capabilities. As technology continues to evolve and as humanity resolves impediments to encryption, future researchers should investigate methods to address this issue. We feel strongly that we must continue to explore these issues in order to protect the critical EAS infrastructure in the US. Nonetheless, organizations working with EASs should encrypt as much as possible and responsibly and proactively.

3.1.3 Regularly Testing Systems

Local EAS officials should also regularly test systems (Fowlkes, 2018) and backup critical data; further, they must change default passwords before connecting to the network to reduce the risk of cyberattacks (Constantin, 2013). EAS owners should establish and enforce a password policy that specifies minimum standards for complexity, change frequency, and password history to prevent reuse of prior passwords. Even after recommending regular password changes, noted cybersecurity researcher Mike Davis told Reuters (2013) that he used Google's search engine and identified at least 30 systems that were vulnerable to attack. If one can view an organization's vulnerabilities with a simple Google search, the organization has not thoroughly tested its systems.

Further, local EAS officials should properly maintain, update, and patch software over time (Wirth, 2017). They should also focus on proper security education, training, and awareness programs to prepare employees and reduce risk (McFarlane, 2017). EAS authorities should have cybersecurity teams in place with a regular plan to evaluate all systems for vulnerabilities (Hub, 2017). However, regular testing involves much challenge to accomplish in practice since few EAS authorities have the necessary funding to thoroughly evaluate systems (Borchert, 2015). Organizations that prioritize threats, use appropriate encryption, and regularly test systems will likely be ready for cybersecurity challenges at least from a technical perspective. However, the most technically capable system may fail if organizations do not recognize social complexities.

3.2 Social Issues and Managerial Challenges

3.2.1 Establishing Coordinated Vulnerability-disclosure (CVD) Policies

It is unrealistic and naïve to assume that EAS authorities can eliminate all vulnerabilities. However, EAS authorities may take several steps to improve security by encouraging cybersecurity researchers to report vulnerabilities they discover. While individuals may report vulnerabilities, McFarlane (2017) recommends that EAS authorities should not overlook crowdsourcing as a valid option wherein they use cybersecurity researchers to identify threats as a supplement their (often limited number of) IT staff. However, in 2015, only six percent of Forbes Global 2000 companies had a method for external cybersecurity researchers to identify, describe, and report vulnerabilities (Branscombe, 2017). Thus, cybersecurity researchers may not know whom to contact regarding vulnerabilities. As a result, efforts to identify vulnerabilities revert to the local, state, federal, and non-government agencies who manage EASs. The current fragmented, non-

standardized, and non-cumulative approach to managing vulnerabilities (DiMase et al., 2015) leads to less than optimal results. An unambiguous, non-fragmented, standardized, and cumulative overall plan to disclose vulnerabilities across all partners in the EAS network would help to overcome threats to system integrity.

Organizations that develop coordinated vulnerability (CVD) policies expand the network of contributors from internal IT professionals to the greater public at large—and cybersecurity researchers in particular—who can identify vulnerabilities and alert the organizations in a coordinated and secure manner. The CVD policy must be clear, however, or cybersecurity researchers will be hesitant to participate. Claus et al. (2015) note that EAS authorities need to keep vulnerability information that people might submit confidential in order to establish trust between them. Moreover, organizations should listen when they receive a valid vulnerability report and address the issue quickly (Davis, 2015). While including cybersecurity researchers in the EAS network adds another layer to the already complex public-private-government partnerships that currently comprise the EAS in the US, the added complexity may be worth the potential gained value.

3.2.2 Public-Private-Government Partnerships

The public-private-government partnerships established for much of the U.S. critical infrastructure systems qualify as an inter-organizational system whose cybersecurity the organizations in the partnerships need to evaluate. Borchert (2015) asserts that corporate security and national security are intertwined. As cloud computing and other distributed systems continue to proliferate, governmental agencies at the federal, state, and local levels must seek partnerships with companies who view cybersecurity as a strategic priority. Moreover, critical cybersecurity recommendations require that government agencies share cyberthreat data, guidelines, and best practices (Claus et al., 2015; Rodin, 2015), and we recommend extending these governance guidelines to all partners in the public-private-government EAS provider network. All partners in the network must understand the interconnected nature of their systems along with the potentially "cascading damages flowing from service outages" (Zeichner, 2001, p. 279). They need to deeply understand how technology in the network interacts interoperates with other elements in the partnership to establish cybersecurity safeguards (Meshkati & Tabibzadeh, 2016).

The EAS in the US has numerous elements in its supply chain, countless vendors, and a lack of consistent cybersecurity standards. In such a situation, organizations cannot easily secure critical infrastructure at all points in the network (Morrison, 2013). While many have recommended public-private-government partnerships to improve the security of critical infrastructures, which includes the EAS (Borchert, 2015; Claus et al., 2015; Eichensehr, 2017; Manley, 2015; Marett, 2015), these partnerships have scarcely practically implemented or tested such infrastructures. Cybersecurity becomes more difficult in these highly complex, interconnected networks. Government agencies with critical infrastructure interests, such as EASs, must evaluate all network members and use the evaluation as a part of the selection process when they choose new vendors; service-level agreements may further specify the levels of cybersecurity expected of all participants in EASs (McFarlane, 2017) with penalties for failure to protect against vulnerabilities.

With the diverse and distributed partnerships in EASs in the US, each partner is only as reliable as the weakest connection in the chain. Cybercriminals will look to illegally access the weakest partner and gain a foothold from which to pivot their attack against other partners in order to achieve their objectives on targets such as EASs. These interconnected networks that include widely dispersed partners that have varying and sometimes competing goals (Eichensehr, 2017) add to the systems' vulnerability. Thus, the partners in the EAS supply chain have to establish a backup plan to minimize their vulnerabilities (Wirth, 2017) and prepare for disaster with resilient systems, particularly when dealing with vital infrastructure systems such as EASs. However, partners can make the best plans not at a high-level with little consultation with other partners but via soliciting feedback and recommendations from users in the EAS network.

3.2.3 Citizens' Direct Involvement

A diverse group, EAS stakeholders have different perspectives and understand how the system should function in different ways. From the government perspective, officials responsible for emergency management and response at the federal, state, and local levels qualify as stakeholders. Publicly broadcast television, radio stations, and cellular telephone providers also qualify as stakeholders. This rich, diverse group possesses varying levels of knowledge relative to their place in the EAS ecosystem.

Stakeholders at the national level will have different perspectives than their state and local counterparts. By coming together, stakeholders at different levels may better understand potential vulnerabilities. Directly involving stakeholders who possess large amounts of local knowledge allows EAS authorities to develop community-centric networks (Baudoin et al., 2016). Stakeholders in these community-centric networks can learn from one another and strengthen the EAS via sharing knowledge with users at different levels of the public-private-government partnership. If EAS authorities develop CVDs as we describe in Section 3.2.1, the network expands to include cybersecurity researchers who, with EAS managers, can synergistically work together to improve the security of vulnerable systems over time. EAS authorities should also draft citizens who are familiar with technology to distribute the word when an emergency occurs. For instance, individuals tweeted and retweeted to quickly and efficiently inform others during a recent tsunami (Chatfield, Scholl, & Brajawidagda, 2013). Similarly, EAS authorities should use other social media platforms to stay up to date on potential security vulnerabilities to learn about potential vulnerabilities through the distributed network and to make decisions during, or even before, cyberattacks (Sheffi, 2015).

While direct citizen involvement during disasters can be helpful, it does not come without concerns. EAS authorities may not have experience interacting with informal leaders and influencers in the affected region (Carley, Malik, Landwehr, Pfeffer, & Kowalchuck, 2016). For instance, during Hurricane Sandy, Chatfield and Reddick (2018) found that, while Twitter use overall benefitted people in the disaster, governments should plan in advance for citizen involvement by creating the necessary policies, structures, and relational mechanisms to enable success. Managers in the public-private-government partnership must seek to secure vulnerable EAS systems, learn over time, involve users in decisions, and use social media wisely. However, without funding, EAS authorities face an almost insurmountable challenge to secure vulnerable systems.

3.2.4 Funding for EASs

Maintaining EASs constitutes a matter of public safety: EAS authorities must provide reliable, accurate, updated, and timely information to the population at risk. Complicating matters, numerous agencies at the federal level jointly manage EASs, such as the Federal Emergency Management Agency, the Federal Communications Commission, and the National Oceanic and Atmospheric Administration. At the local, state, city, and county levels, numerous other agencies coordinate budgeting for relevant EASs; thus, finding precise budgeted versus actual expenditures remains elusive. However, EAS authorities often lack funding to invest in cybersecurity and evaluate their systems (Hub, 2017; McFarlane, 2017). Borchert (2015) encourages lawmakers to pursue legislation while encouraging stakeholders to self-regulate. However, EAS authorities cannot easily self-regulate without adequate funding.

3.3 Need for System Resilience

While organizations should be as secure as possible, they cannot eliminate vulnerabilities; instead, partners throughout the EAS network should be able to detect vulnerabilities and respond to them quickly (Sheffi, 2015). Organizations and partners should build resilience and the ability to recover from disaster into the overall cybersecurity plan (Borchert, 2015; Collier & Lakoff, 2015; DiMase et al., 2015; Egli, 2013; Karlsson, Kolkowska, & Prenkert, 2016; Peeters, 2017; Jung & Song, 2015). The U.S. Navy's U.S. Fleet Cyber Command agrees and has called for cyber resilience strategies and sustainable networks when an attack occurs for any branch of the armed services (Cronk & Staten, 2018). Resilient systems do not reduce all threats just as adequately funded and adept cybersecurity policies implemented throughout the EAS provider network will not reduce all threats. However, resilient systems reduce the impact of threats on the system as a whole and the cascading threats throughout the network (Tagarev, Sharkov, & Stoianov, 2017).

Complicating the matter, one cannot easily define resilience, and, indeed, when analyzing their recovery strategies and processes, partners often focus only on their portion of the system. Thus, the research on risk management for emergency alert systems and network resilience at large has become somewhat fragmented and non-cumulative (DiMase et al., 2015; Egli, 2013; Meshkati & Tabibzadeh, 2016) with poor understanding of the complex cybersecurity issues that arise throughout the interconnected enterprises (DiMase et al., 2015). With many such public-private-government connections throughout the critical infrastructure of the EAS, different groups often define resilience in their own way with little coordination. In contrast, we define resilience in the highly interconnected U.S. EAS as a set of planned and coordinated processes across organizations that have specified roles and responsibilities to protect,

defend, and recover EASs (Raab, Jones, & Székely, 2015) and the ability to communicate emergency information and alerts to populations at the federal, state, and local levels. Building on EASs' interconnected nature, Egli (2013) goes further in viewing resilience "as a public good enabled by collective action, interagency coordination, and public-private partnerships" (p. 32). Wrona et al. (2018) concur in advocating for a "fail fast" option where organizations embrace failures and learn from them to improve security and resilience over time. However, some authors have cautioned organizations not to fall into the cybersecurity paradox in which they strengthen infrastructure at the expense of individual privacy rights. Instead, these authors recommend that organizations secure their infrastructure and build resilience while ensuring that they protect individual privacy (Dunn-Cavelty, 2014; Raab et al., 2015). Resilient organizations may find it easier to recover from cybersecurity failures that occur on networks with which they connect. Given that emergency networks often connect with many others throughout and across the supply chain, the network is only as safe as the least safe system in the integrated and interconnected system (Meshkati & Tabibzadeh, 2016).

Moreover, since private organizations own and operate most EASs (Borchert, 2015; Egli, 2013), they tend to focus on their own immediate needs and may not consider the importance of interconnectivity. However, these organizations need to connect with others, particularly in large-scale disasters that span multiple cities, counties, localities, states, and even countries. Integrated command centers, perhaps with liaisons at each organizational unit (Claus, Gandhi, Rawnsley, & Crowe, 2015), may reduce the impact and increase the resiliency of the emergency system's interconnected network while increasing the effectiveness of the response. Since almost 75 percent of the U.S. population lives in 11 mega-regions (Todorovich, 2008), a well-positioned interconnected network that remains resilient in the face of disaster could serve a large portion of the US. Liaisons in these 11 mega-regions could coordinate with the local, state, regional, and federal EAS authorities to improve preparation for and reaction to a security disaster.

The EAS in the US faces a daunting cybersecurity challenge in reducing system vulnerabilities across every region, state, city, county, and municipality. No easy fix exists, and vulnerabilities may vary from location to location. However, to evaluate the cybersecurity challenges that the EASs in the US face, we reviewed EASs' current open availability and vulnerability-disclosure policies in organizations in the Southeastern US.

4 Method

We searched for Internet-accessible EAS management websites from six southeastern states to determine whether one could access them via either the Hypertext Transfer Protocol (HTTP) or the Hypertext Transfer Protocol Secure (HTTPS). To do so, we used the Shodan application (see https://www.shodan.io/), a publicly available application that indexes search results for websites, networked devices, and so on with details pertinent to security researchers (Barnaghi & Sheth, 2016; Konstantinou, Sazos, & Maniatakos, 2016; Serbanescu, Obermeier, & Yu, 2015). However, using data from the Shodan application has its concerns. As Konstantinou et al. (2016) note, it remains unclear how frequently the Shodan application scans the Internet for new data and how often it indexes those results for public access.

In 2018, we began the data-collection process. Initially, we hoped to identify EAS management websites from numerous vendors. In addition to the DAS/ME websites, we located websites for EAS technology products by Everbridge, Inspiron Logistics, and Vesta Public Safety (formerly known as Cassidian Communications). However, these websites did not provide enough information to determine which municipality used them, which prevented further analysis. The DAS/ME websites, however, did provide enough detail to gather and analyze. Since sources have reported DAS/ME as "the global leader in emergency communications solutions" (Dundee Hills Group, 2018) and a leader in the EAS industry (Monroe Electronics, n.d.; Reuters, 2013; Storm, 2013), we used DAS/ME for our analysis.

Using Shodan, we conducted a search query and collected the results returned. Next, we further evaluated each website before including it in our study. First, we visited each website and determined if it met our specific definition as an Internet-accessible EAS management interface website. During this process, we also eliminated duplicate instances (e.g., where our results already included a specific municipality). In some cases, we ultimately identified 20 or more websites that Shodan returned as belonging to only one EAS system. Nevertheless, we had to carefully check and analyze each website to decide whether to include it in our study.

Then, after locating and confirming that a particular EAS met our definition, was linked to a specific municipality, and was not a duplicate, we more deeply searched for coordinated vulnerability-disclosure (CVD) policies for the specified websites, a time-consuming and complex task. Thus, based on the non-trivial nature of the analysis we needed to perform for each website that Shodan identified, we chose to focus on a manageable sample. We gathered data from six southeastern states: Alabama, Florida, Georgia, North Carolina, South Carolina, and Tennessee. With almost 60 million residents in these six states compared to just under 330 million in the United States as a whole (U.S. Census Bureau, 2019), we believe our sample provides a suitable surrogate from which to draw initial recommendations for EASs in the U.S.

Given the identified guidelines, we searched for Internet-accessible EAS management websites in six southeastern states. Shodan provides several items of interest, such as IP address, TLS encryption details (when websites enabled encryption), and the city name associated with the IP address. We then aggregated the search results into a spreadsheet for further analysis.

Next, we had student researchers manually visit each EAS management website that Shodan outputted using a Web browser. During this phase, the student researchers collected additional data. In particular, they collected the displayed website name, municipality name when displayed, EAS serial number, and platform ID, analog and digital transmitter details, and the date/time the student researchers accessed the website. Note that that the EAS management websites had this information on their login page: the student researchers took no additional steps other than to visit the IP address using a Web browser. We conducted no further reconnaissance on the EAS management websites outside the Shodan results and the login pages. At no time did anyone associated with this research effort engage in any attempt to log in to any of the EAS management websites. Finally, at no time did anyone associated with this research engage in any offensive activities in order to gain access to any of the EAS management websites. We all agreed that we would not attempt to log into any of the EAS management websites since we lacked the authorization to do so.

5 Results

5.1 Internet-accessible EAS Management Websites

Internet-accessible EAS management websites pose a severe vulnerability to their owners. All Internet-accessible systems represent potential targets for brute-force attacks wherein cybercriminals try various username and password combinations to gain unauthorized access. Once cybercriminals gain access to an EAS management website, they could choose to change basic system configuration options (e.g., radio frequencies used to broadcast messages), trigger warning sirens, send fake alerts, cancel existing valid alerts, disrupting the ability to send alerts completely, and so on. Such actions could mean the difference between life and death for people in the relevant geographic areas; thus, cybersecurity professionals who design, maintain, and secure EASs must be very confident that the systems will work as intended. We cannot accept lost life due to a compromised system. Our analysis yielded 18 Internet-accessible EAS management websites across the Southeastern United States (see Table 2).

Table 2. States and Number of Internet-accessible EAS Management Websites

State	Number of Internet-accessible websites
Alabama	4
Florida	1
Georgia	4
North Carolina	2
South Carolina	2
Tennessee	5
Total	**18**

5.2 Vulnerability-disclosure Policies

None of the 18 Internet-accessible EAS management websites had a process in place for cybersecurity researchers to report vulnerabilities. We intended to inform the appropriate EAS authorities about the vulnerabilities in their respective systems, but we found public method that we could undertake to do so.

Historically, vulnerability-disclosure policies have provided ways for cybersecurity researchers to inform companies of vulnerabilities discovered in their software products. However, all organizations face vulnerabilities and their associated risks, not just companies that develop software; similarly, anyone (not just cybersecurity researchers) may discover vulnerabilities.

Our research into EAS management websites highlights a vulnerability that exists not due to a flaw in an application but due to how organizations chose to implement an application in their network. For instance, some EAS providers have ignored the specific advice from DAS/ME and not changed the admin password when they installed a system. Users or cybersecurity researchers could have alerted the EASs to this error, but they had no way to report an implementation vulnerability. Thus, we propose that all organizations should have vulnerability-disclosure programs in place regardless of whether or not they develop applications; further, vulnerability-disclosure programs should be publicly available so that anyone—cybersecurity researcher or not—may report a vulnerability.

6 Analysis of Results

6.1 Internet-accessible EAS Management Websites

Of the six states we investigated, all had at least one Internet-accessible EAS management website interface. Multiple websites offered access using HTTP, which poses some concern since HTTP does not encrypt traffic, which means anyone who can capture it can read it. Tennessee led the way with five Internet-accessible EAS management websites, while Alabama and Georgia had four each. North Carolina and South Carolina had two each, and Florida followed with one. For an essential component of the U.S. national infrastructure, we contend that individuals should not openly be able to access EAS management websites at all on the Internet with a simple user identification and password.

We found at least one weak link in all the six states we analyzed. That one weak link may compromise the entire EAS network. Even someone with minimal technical skills could accidentally land at one of these Internet-accessible EAS management websites. By following the technical and management guidelines we recommend, EAS authorities may minimize the threats due to vulnerabilities. By regularly testing systems and using Shodan or other Internet-scanning applications, EAS owners can avoid overlooking vulnerabilities. In testing systems, EAS owners should also verify that they use no default passwords.

EAS authorities must argue for and carefully justify the funding that they need. Moreover, government agencies must be sensitive to burdensome administrative requirements and make the process as easy as possible for the EAS network's members and allow them to electronically fill EAS risk-management plans much like the Alert Reporting System (ARS) that the FCC recently implemented (RadioResource, 2018). EAS authorities at all levels should seek ways to reduce burdensome requirements and allow organizations in the supply chain to focus on cybersecurity initiatives to strengthen the system as a whole. While the ARS represents a step in the right direction, EAS authorities should investigate other opportunities as well.

Since funding will likely remain in short supply, we encourage EAS authorities to consider using highly trained cybersecurity professionals to help them find vulnerabilities. EAS authorities should also closely monitor social media and the cybersecurity community. For instance, if users note concerns with receiving false or misleading EAS messages, they will likely post on social media and, thus, give EAS authorities information that could alert them to a problem with their systems. Also, EAS authorities should monitor cybersecurity forums for evidence of system vulnerabilities. Our paper highlights how individuals who lead the cybersecurity efforts in the EAS network need technical and social skills and to implement appropriate management policies.

6.2 Vulnerability-disclosure Policies

As cybersecurity researchers, we wanted to disclose the vulnerabilities we identified in each state. However, since no entity with an Internet-accessible EAS management website had a published method

to report the vulnerability, we had no clear process to follow in our attempts to report the cybersecurity concerns. Moving to a higher level, we also examined the state EAS websites, which, as of February, 2018, offered no path to report vulnerabilities. Thus, we find it unsurprising that other entities lower in the EAS supply chain failed to provide a method to report vulnerabilities. We encourage providers in the EAS network to publish a vulnerability-disclosure process. At the least, such a process would allow free cybersecurity help; at the most, it may encourage testing beyond what each entity can undertake itself due to inadequate funding.

The cybersecurity professional network represents an untapped resource that could help to secure and protect EASs. However, when EAS authorities do not have vulnerability-disclosure policies in place, cybersecurity researchers cannot report directly to the affected entity in the EAS supply chain. Instead, researchers may give up on reporting vulnerabilities. Alternatively, they may report it publicly to incentivize the system owners to address the vulnerability. Unfortunately, disclosing the vulnerability in an uncoordinated way may make a system even less secure until its owner develops a mitigation strategy. However, if local, city, county, state, and federal emergency management authorities publish a way to report vulnerabilities, they could resolve problems quietly and eventually disclose them in a coordinated way (after they mitigated them). In doing so, they could give the individual(s) responsible for discovering it credit and allow the critical infrastructure in the US to continuously improve.

EAS authorities must publish a way for cybersecurity researchers to report vulnerabilities without fear of reprisal. While we recommend they create CVD policies, any easy to find vulnerability policy would be better than what exists now. We further recommend that the policy explicitly absolves anyone who reports the vulnerability of any legal or civil penalties as long as individuals only locate and disclose the vulnerability as the policy specifies and do not attack the system with it. Since the network comprises numerous public, private, and governmental organizations that own EAS assets, they must coordinate with one another when developing a policy on vulnerability disclosure (i.e., up, down, and across the supply chain). Otherwise, cybercriminals will likely exploit any discovered vulnerabilities and, thus, potentially compromise the entire EAS network.

We do not identify the Internet-accessible EAS management websites that we discovered. Some no longer exist, while new ones may have emerged. We strongly encourage all EAS authorities to provide a proper method to report identified vulnerabilities. Cybersecurity researchers want to help; companies should allow them to do so.

6.3 Restricting Access to EAS Management Websites

EAS management websites constitute an essential component in delivering alerts to the public. These websites allow authorized users to manage EAS systems and send alerts remotely, a critical capability when time matters. However, we argue that having these websites directly accessible from the Internet poses an unnecessary risk and potentially exposes the public to false alerts or prevents EAS authorities from delivering actual emergency alerts.

To mitigate this risk, we propose a multi-step technical solution for EAS owners. First, we propose that they place their EAS management websites in their internal network and, thus, remove the ability for someone to directly access it via the Internet. Next, we propose they place the website on a virtual local area network (VLAN) segment in their internal network to further restrict access to the EAS management website to specific IP addresses in the internal network. VLANs represent a common networking control to protect sensitive systems from unauthorized access (Kiravuo, Sarela, & Manner, 2013). Furthermore, we propose that organizations allow remote access to the VLAN segment via a virtual private network (VPN) so that one can access the EAS remotely if needed as the National Institute of Standards and Technology (NIST) recommends (Frankel et al., 2005). We propose restricting VPN access to defined VLANs and limiting access based on authorization to use the EAS management website and transmit alerts. Next, we propose that EAS authorities implement multifactor authentication (MFA) in conjunction with VPN access in order to further improve their overall security posture (Jakimoski, 2016). Also, they could configure VPN user authentication to deny access from IP addresses not from the US (also known as geo-blocking) (Taylor, Devlin, & Curran, 2012). We concede that user authentication has limited effectiveness due to the relative ease and availability with which one can use proxy servers (Edelman, 2015), but as part of an overall layered technical risk management plan, it may be useful.

We also propose technical solutions for EAS manufacturers to build into their products that would help their customers maintain a more robust security posture. First, we propose that EAS manufacturers build

in a mandatory administrator (admin) password change as part of the initial setup. System documentation on EAS manufacturers' websites often contain EAS default admin passwords, which anyone who does a quick Google search can easily access. Forcing a change of the default password during initial setup would prevent EAS owners from leaving default admin passwords in place after setup. Next, we propose that EAS manufacturers build MFA controls into their product. Finally, we propose that EAS manufacturers build rules into their setup and configuration that would require system owners to place the EAS management website interface on a private network address and, thus, remove the possibility of ever attaching it directly to the Internet.

6.4 Overall Recommendations

Throughout the EAS network, EAS authorities should prioritize threats with consistent policies that maximize the entire EAS network's security rather than use individually developed, decentralized, and fragmented plans. We also recommend they regularly test EASs in a structured and standardized manner to avoid the chance they will use default passwords, for instance; we recommend continuous system testing to ensure high levels of cybersecurity preparedness. To accomplish these technical goals, partners in the EAS supply chain should cultivate relationships with one another and allow citizens to become involved. Since we realize that one cannot ever fully prevent vulnerabilities even with proper planning, we recommend that members in the EAS supply chain publish a set of vulnerability-disclosure policies that cybersecurity professionals who may find and want to report potential problems can use. For EAS providers who fail to follow technical guidelines and managerial strategies, an insecure network and cybercriminals will likely compromise the network. While most known attacks on EASs have not resulted in problems with distributing valid warnings, the future remains uncertain. EAS providers should seek to lead the way with high-quality technical security and managerial policies that secure the network while still providing convenience for authorized parties to use the decentralized systems. With cybercriminals from other countries attempting to infiltrate elections systems, email servers, and the like, we can reasonably assume that cybercriminals have tried—and will keep trying—to infiltrate EASs as a method to disrupt one of the critical infrastructure systems in the US.

7 Limitations and Future Research

Our study has several limitations. First, future research needs to generate and test the theoretical foundations of potential vulnerabilities in EASs in the US. We describe methods to improve resilience and increase the security of only one particular critical infrastructure system, the EAS. Future researchers will no doubt find it challenging to test the resilience and vulnerability of EASs due to the secrecy shrouding critical governmental infrastructure (Karlsson, Kolkowska, & Prenkert, 2016). Also, while we recommended EAS authorities encrypt EAS data, no good solution currently to encrypt data at rest and in motion exists; thus, future researchers will have to evaluate this issue as encryption research advances.

Further, if cybersecurity researchers do decide to test EASs for potential vulnerabilities, they may face severe civil and criminal consequences, an area that deserves future research. Additionally, our research may not generalize to EASs outside the US since other countries may have specific contextual factors that differ from the EASs that we discuss here (Ochara, 2017). Similarly, other regions in the US may have different characteristics than the Southeastern US that we examined. Our decision to examine systems from DAS/ME also limits our research. While we identified Internet-accessible EAS management websites for products that other providers made, beyond DAS/ME, they lacked sufficient detail to allow one to determine which municipality used them. As a result, we only included DAS/ME for our analysis. However, DAS/ME is a leader in EASs, and news reviews often mention it; thus, we believe that DAS/ME represents a practical, relevant, and appropriate choice to examine.

While we made several recommendations to secure vulnerable EASs, one should not overlook other technical limitations. For instance, 2G technology, which still sees wide use and has weak mobile security, has unavoidable security vulnerabilities (Jøsang, Miralabé, & Dallot, 2015). EAS authorities must carefully consider vulnerabilities in the technology itself and in the capabilities of rapidly developing mobile capabilities with a clear plan to mitigate such vulnerabilities. Furthermore, reliance on Shodan has limitations, and we encourage researchers to use other tools and compare performance among and between applications.

Moreover, while we recommended EAS authorities to adopt cybersecurity policies to prevent system vulnerabilities, we did not survey end users as other researchers have recommended (Karlsson,

Kolkowska, & Prenkert, 2016). Since end users ultimately make the system work, assessing their attitudes and perceptions about system vulnerabilities and gathering their input into possible remedies would be informing. Moreover, while previous researchers have noted the importance of adequately training employees in security techniques, we did not investigate the impact of training on how EAS authorities develop, implement, and enforce cybersecurity policies for vulnerable systems. We encourage other researchers to study this area, which falls outside our scope here.

Our focus on EASs in particular may limit our recommendations' external generalizability. Work that analyzed vulnerability and resilience in other U.S. critical infrastructures, such as the water system and the electric grid, might lend further insight into how organizations can use management policies to improve the resilience of the interconnected network of technological systems that keep the water running and the lights on. Further, since private organizations own most portions of critical infrastructure, understanding how small—but crucial—portions of critical infrastructure work would add to the network of associations and clarify the interrelationships between public-private-governmental partnerships.

Finally, we did not communicate with EAS owners or local and state agencies since no website we analyzed posted a CVD policy; in fact, we never found a point of contact to alert about the vulnerability in the EAS even if we had dared to report the vulnerability. Our unwillingness to report rests on our fearing either criminal or civil repercussions as has happened with cybersecurity researchers in the past (Doctorow, 2017; Gallagher, 2019; Goodin, 2016). If we had found a CVD policy and if we could easily access a point of contact, we would have followed through and notified the specific municipalities of their potential insecurities. We do, however, encourage all providers in the EAS supply chain to use Shodan or other free tools to quickly identify if they may be vulnerable.

8 Conclusion

To date, no research has specifically evaluated the cybersecurity of U.S. EASs and recommended strategies to secure the systems. Our work provides two contributions to the research and practitioner communities. First, we present a snapshot of current EASs in the Southeastern US and report on the number of Internet-accessible EAS management websites; our results confirm continued cybersecurity vulnerabilities even after much-disclosed, publicly embarrassing breaches in the past. As such, they should spur all EAS managers to investigate the cybersecurity of the systems they manage. Further, EASs lack publicly available coordinated vulnerability-disclosure policies, which would allow cybersecurity researchers to report potential problems without fear of legal repercussions; thus, we conclude that organizations should develop such policies and possibly incentivize individuals who detect and report potential cybersecurity risks. With ongoing reports of demonstrated cybersecurity challenges in EASs, this study provides EAS managers with clearly identifiable steps that they make take to secure the systems they manage. Moreover, as the first academic work to evaluate the current security posture of EASs and recommend countermeasures that EAS authorities should consider, we see future research opportunities that could expand to other critical infrastructures at the regional, city, state, national, and even international levels.

We must secure EASs and be able to inform affected groups when true emergencies occur. The EAS as a whole must be resilient, and authorities need to recognize that unintended vulnerabilities will occur but ensure that individual EASs can bounce back quickly. The entire system is only as strong as the weakest link. A bottom-up approach to develop resilience that starts at the local level and moves to the state, for instance, represents one option. A top-down approach in which the country or states take the lead and move down to the local, city, and county municipalities represents another. We argue that EAS authorities must do something, and they must do it now. Our aging, vulnerable EASs cannot handle potential threats, and we lack sufficient budgets to find all vulnerabilities in the first place. Closing all access to EASs openly available on the Internet constitutes an easy way to strengthen the U.S. EAS, which benefits society as a whole. With a strong EAS cybersecurity plan in place, which includes proper risk management, CVD policies, data encryption where possible, system testing, sufficient funding, strong private-public-government partnerships, end-user training, and threat prioritization, the EAS in the US will become more resilient and, thus, provide valid, accurate, and timely information to people. The number of cybercriminals attacking EASs will only increase; however, resilient EASs and EAS authorities that respond appropriately and according to their cybersecurity plans will prevent malicious parties from accessing them.

References

Albanesius, C. (2013). Emergency alert system vulnerable to hackers, report finds. *PC Magazine*. Retrieved from https://www.pcmag.com/article2/0,2817,2421503,00.asp

Barnaghi, P., & Sheth, A. (2016). On searching the internet of things: Requirements and challenges. *IEEE Intelligent Systems*, *31*(6), 71-75.

Baudoin, M. A., Henly-Shepard, S., Fernando, N., Sitati, A., & Zommers, Z. (2016). From top-down to "community-centric" approaches to early warning systems: Exploring pathways to improve disaster risk reduction through community participation. *Science*, *7*(2), 163-174.

Borchert, H. (2015). It takes two to tango: Public-private information management to advance critical infrastructure protection. *European Journal of Risk Regulation*, *6*(2), 208-218.

Branscombe, M. (2017). How to handle security vulnerability reports. *CIO*. Retrieved from https://www.cio.com/article/3157698/security/how-to-handle-security-vulnerability-reports.html

Carley, K. M., Malik, M., Landwehr, P. M., Pfeffer, J., & Kowalchuck, M. (2016). Crowd sourcing disaster management: The complex nature of Twitter usage in Padang Indonesia. *Safety Science*, *90*, 48-61.

Chatfield, A. T., & Reddick, C. G. (2018). All hands on deck to tweet #sandy: Networked governance of citizen coproduction in turbulent times. *Government Information Quarterly*, *35*(2), 259-272.

Chatfield, A. T., Scholl, H. J., & Brajawidagda, U. (2013). Tsunami early warnings via Twitter in government: Net-savvy citizens' co-production of time-critical public information services. *Government Information Quarterly*, *30*(4), 377-386.

Claus, B., Gandhi, R. A., Rawnsley, J., & Crowe, J. (2015). Using the oldest military force for the newest national defense. *Journal of Strategic Security*, *8*(4), 1-22.

Collier, S. J., & Lakoff, A. (2015). Vital systems security: Reflexive biopolitics and the government of emergency. *Theory, Culture, & Society*, *32*(2), 19-51.

Constantin, L. (2013). Emergency alert system devices vulnerable to hacker attacks, researchers say. *ComputerWorld*. Retrieved from https://www.computerworld.com/article/2494934/malware-vulnerabilities/emergency-alert-system-devices-vulnerable-to-hacker-attacks--researchers-say.html

Cronk, T. M., & Staten, D. (2018). Military officials testify on cybersecurity on Capitol Hill. *U.S. Department of Defense*. Retrieved from https://www.defense.gov/News/Article/Article/1466442/

Davis, M. (2015). Developers: How do you respond to security researcher's vulnerability reports? *Future Hosting*. Retrieved from https://www.futurehosting.com/blog/developers-how-do-you-respond-to-security-researchers-vulnerability-reports/

Demer, L. (2018). Alaska emergency alert system less vulnerable to false alarms than Hawaii's, officials believe. *Anchorage Daily News*. Retrieved from https://www.adn.com/alaska-news/military/2018/01/15/alaska-officials-think-the-states-emergency-system-avoids-false-alarms-like-in-hawaii/

DiMase, D., Collier, Z. A., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions*, *35*(2), 291-300.

Doctorow, C. (2017). Security researcher arrested after he warns Hungarian transit company about their dumb mistake. *Boingboing*. Retrieved from https://boingboing.net/2017/07/24/hungarian-messenger-shooting.html

Dodril, T. (2016). Emergency alert system vulnerabilities could allow terrorists to manipulate a disaster. *SurvivalBased.* Retrieved from http://www.survivalbased.com/survival-blog/7229/emergency-alert-system-vulnerabilities-could-allow-terrorists-to-manipulate-a-disaster/

Dreyfuss, E. (2018). Why didn't I get an emergency Presidential alert text? *Wired.* Retrieved from https://www.wired.com/story/why-didnt-i-get-emergency-presidential-alert-text/

Dundee Hills Group. (2018). Monroe Electronics to demonstrate industry-first advancements in emergency alert monitoring, management, and compliance at SCTE Cable-Tec Expo 2018.

Lyndonville, NY. *Multichannel*. Retrieved from https://www.multichannel.com/pr-feed/monroe-electronics-to-demonstrate-industry-first-advancements-in-emergency-alert-monitoring-management-and-compliance-at-scte-cable-tec-expo-2018

Dunn-Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701-715.

Edelman, M. (2015). The thrill of anticipation: Why the circumvention of geoblocks should be illegal. *Virginia Sports & Entertainment Law Journal*, *15*, 110-134.

Egli, D. S. (2013). Beyond the storms: Strengthening preparedness, response, & resilience in the 21st century. *Journal of Strategic Security*, *6*(2), 32-45.

Eichensehr, K. E. (2017). Public-private cybersecurity. *Texas Law Review*, *95*(3), 467-538.

Faris, D. (2018). Why Hawaii's false alarm should be a massive wake-up call for us. *The Week*. https://theweek.com/articles/748499/why-hawaiis-false-alarm-should-massive-wakeup-call-all

Federal Communications Commission. (2018). *Emergency alert system*. Retrieved from https://www.govinfo.gov/content/pkg/FR-2018-08-02/pdf/2018-15818.pdf

Federal Communications Commission. (n.d.). *Emergency alert system (EAS).* Retrieved from https://www.fcc.gov/general/emergency-alert-system-eas

FEMA. (2007). *Emergency alert system and notification.* Retrieved from https://web.archive.org/web/20070717212239/http://www.fema.gov/media/fact_sheets/eas.shtm

Fiat, A., & Naor, M. (1993). Broadcast encryption. In *Proceedings of the 13th Annual International Cryptology Conference.* Retrieved from https://www.iacr.org/cryptodb/data/paper.php?pubkey=1293

Fletcher, M. J. (2016a). The emergency alert system test: Lesson learned, catastrophe averted. *Network World*. Retrieved from https://www.networkworld.com/article/3125754/mobile-wireless/the-emergency-alert-system-test-lesson-learned-catastrophe-averted.html#tk.drr_mlt

Fletcher, M. J. (2016b). The emergency alert system: Failure IS an option. *NetworkWorld*. Retrieved from https://www.networkworld.com/article/3123778/mobile-wireless/the-emergency-alert-system-failure-is-an-option.html

Fowlkes, Lisa M. (2018). Emergency alert testing matters. *Federal Communications Commission.* Retrieved from https://www.fcc.gov/news-events/blog/2018/10/02/emergency-alert-testing-matters

Frankel, S. E., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W., & Sharma, S. R. (2005). Guide to IPsec VPNs. *NIST*. Retrieved from https://doi.org/10.6028/NIST.SP.800-77

Gallagher, S. (2019). Casino screwup royale: A tale of “ethical hacking” gone awry. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2019/03/50-shades-of-greyhat-a-study-in-how-not-to-handle-security-disclosures/

Goodin, D. (2016). Armed FBI agents raid home of researcher who found unsecured patient data. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2016/05/armed-fbi-agents-raid-home-of-researcher-who-found-unsecured-patent-data/

Halevy, D., & Shamir, A. (2002). The LSD broadcast encryption scheme. In *Proceedings of the 22nd Annual International Cryptology Conference.*

Hemme, K. (2015). Critical infrastructure protection: Maintenance is national security. *Journal of Strategic Security, 8*(5), 25-39.

Hub. (2017). Hackers put the entire city of Dallas on alert. *Hub*. Retrieved from https://www.hubinternational.com/blog/2017/04/hackers-put-the-entire-city-of-dallas-on-alert/

Jakimoski, K. (2016). Security techniques for data protection in cloud computing. *International Journal of Grid and Distributed Computing*, *9*(1), 49-56.

Jøsang, A., Miralabé, L., & Dallot, L. (2015). Vulnerability by design in mobile network security. *Journal of Information Warfare*, *14*(4), 85-97.

Jung, K., & Song, M. (2015). Linking emergency management networks to disaster resilience: Bonding and bridging strategy in hierarchical or horizontal collaboration networks. *Quality and Quantity*, *49*(4), 1465-1483.

Kang, C. (2018). False missile warning in Hawaii adds to scrutiny of emergency alert system. *The New York Times.* Retrieved from https://www.nytimes.com/2018/01/13/business/hawaii-missile-emergency-alert.html

Karlsson, F., Kolkowska, E., & Prenkert, F. (2016). Inter-organisational information security: A systematic literature review. *Information and Computer Security*, *24*(5), 418-451.

Kiravuo, T., Sarela, M., & Manner, J. (2013). A Survey of Ethernet LAN Security. *IEEE Communications Surveys & Tutorials*, *15*(3), 1477-1491.

Konstantinou, C., Sazos, M., & Maniatakos, M. (2016). Attacking the smart grid using public information. In *Proceedings of the 17th Latin-American Test Symposium.*

Lanier, C. (2018). Critical infrastructure & supply chain remain highly vulnerable to attacks. *BleepingComputer.* Retrieved from https://www.bleepingcomputer.com/news/security/critical-infrastructure-and-supply-chain-remain-highly-vulnerable-to-attacks/

Li, D. C. (2015). Online security performances and information security disclosures. *The Journal of Computer Information Systems*, *55*(2), 20-28.

Lotspiech, J., Nusser, S., & Pestoni, F. (2002). Broadcast encryption's bright future. *IEEE Computer*, *35*(8), 57-63.

Loukas, G., Gan, D., & Tuan, V. (2013). A taxonomy of cyber attack and defence mechanisms for emergency management networks. In *Proceedings of the 2013 IEEE International Conference on Pervasive Computing and Communications Workshops.*

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. *Journal of Strategic Security*, *8*(3), 85-98.

Marett, K. (2015). Checking the manipulation checks in information security research. *Information and Computer Security*, *23*(1), 20-30.

Matthews, W. (2014). Cyber uncertainty. *National Guard*. Retrieved from http://nationalguardmagazine.com/article/Cyber_Uncertainty/1764536/218066/article.html

McFarlane, R. (2017). Hacking emergency services: How safe is the 911 system? *GCN*. Retrieved from https://gcn.com/articles/2017/07/18/hacking-emergency-services.aspx

Meshkati, N., & Tabibzadeh, M. (2016). An integrated system-oriented model for the interoperability of multiple emergency response agencies in large-scale disasters: Implications for the Persian Gulf. *International Journal of Disaster Risk Science*, *7*, 227-244.

Metivier, B. (2017). Fundamental objectives of information security: The CIA triad. *Sage Data Security*. Retrieved from https://www.sagedatasecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad

Monroe Electronics. (n.d.). *About Monroe Electronics.* Retrieved from https://www.monroe-electronics.com/me_about.html

Morrison, M. I. (2013). The acquisition supply chain and the security of governmental information technology purchases. *Public Contract Law Journal*, *42*(4), 749-792.

Morss, R. E., Demuth, J. L., Bostrom, A., Lazo, J. K., & Lazrus, H. (2015). Flash flood risks and warning decisions: A mental models study of forecasters, public officials, and media broadcasters in Boulder, Colorado. *Risk Analysis*, *35*, 2009-2028.

Nixon, R. (2016). Homeland Security Dept. struggles to hire staff to combat cyberattacks. *The New York Times*. Retrieved from https://www.nytimes.com/2016/04/07/us/politics/homeland-security-dept-struggles-to-hire-staff-to-combat-cyberattacks.html

Ochara, N. M. (2017,). Assessing irreversibility of an e-government project in Kenya: Implication for governance. *Government Information Quarterly*, *27*(1), 89-97.

Ollmann, G. (2013). Hacking the emergency alerting system. *Dark Reading*. Retrieved from https://www.darkreading.com/attacks-breaches/hacking-the-emergency-alerting-system/d/d-id/1140113

Pallotta, F. (2014). Cable customers startled by "emergency alerts". *CNN*. Retrieved from http://money.cnn.com/2014/10/24/media/att-alerts/index.html

Peeters, G. (2017). *Strengthening the Achilles heel of the European Union: Make use of ethical hackers to find vulnerabilities in information systems (*master's thesis)? Leiden University. Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/55426/Masterthesis%20Gijs%20Peeters%20S1584103%20%5bJuly%202017%20final%5d.pdf?sequence=1

Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. *Media and Communication*, *3*(2), 21-41.

RadioResource. (2018). *FCC creates new reporting system for emergency alerts.* Retrieved from https://www.rrmediagroup.com/News/NewsDetails/NewsID/16729

Reuters. (2013). Zombie hack blamed on easy passwords. *Chicago Tribune*. Retrieved from http://articles.chicagotribune.com/2013-02-14/business/chi-zombie-hack-blamed-on-easy-passwords-20130214_1_karole-white-ioactive-labs-passwords

Roberts, P. (2013). Emergency alert system: Vulnerable systems double, despite zombie hoax. *The Security Ledger.* Retrieved from https://securityledger.com/2013/07/emergency-alert-system-vulnerable-systems-double-despite-zombie-hoax/

Rodin, D. N. (2015). The cybersecurity partnership: A proposal for cyberthreat information sharing between contractors and the federal government. *Public Contract Law Journal*, *44*(3), 505-528.

Schulzrinne, H., & Arabshian, K. (2002). Providing emergency services in Internet telephony. *IEEE Internet Computing*, *6*(3), 39-47.

Seddigh, N., Nandy, B., & Lambadaris, J. (2006). An internet public alerting system: A Canadian experience. In *Proceedings of the 3rd International ISCRAM Conference.*

Serbanescu, A. V., Obermeier, S., & Yu, D.-Y. (2015). A flexible architecture for industrial control system honeypots. In *Proceedings of the 12th International Joint Conference on e-Business and Telecommunications.*

Sheffi, Y. (2015). Preparing for disruptions through early detection. *MIT Sloan Management Review*, *57*(1), 31-42.

Shu, G., Lee, D., & Yannakakis, M. (2006). A note on broadcast encryption key management with applications to large scale emergency alert systems. In *Proceedings of the 20th IEEE International Parallel & Distributed Processing Symposium.*

Sidner, S., & Andone, D. (2018). What went wrong with Hawaii's false emergency alert? *CNN*. Retrieved from https://www.cnn.com/2018/01/14/us/hawaii-false-alarm-explanation/index.html

Storm, D. (2013). Hackers can hijack unpatched emergency alert system devices, broadcast bogus warnings. *ComputerWorld*. Retrieved from https://www.computerworld.com/article/2473992/malware-vulnerabilities/hackers-can-hijack-unpatched-emergency-alert-system-devices--broadcast-bogus.html

Tagarev, T., Sharkov, G., & Stoianov, N. (2017). Cyber security and resilience of modern societies: A research management architecture. *Information & Security*, *38*, 93-108.

Taylor, J., Devlin, J., & Curran, K. (2012). Bringing location to IP addresses with IP Geolocation. *Journal of Emerging Technologies in Web Intelligence*, *4*(3), 273-277.

Todorovich, P. (2008). America 2050: An infrastructure vision for 21st Century America. *Regional Plan Association.* Retrieved from http://www.america2050.org/pdf/2050_Report_Infrastructure_2008.pdf

U.S. Census Bureau. (2019). *National population totals and components of change: 2010-2019.* Retrieved from https://www.census.gov/data/tables/time-series/demo/popest/2010s-national-total.html

Wentz, B., Lazar, J., Stein, M., Gbenro, O., Holandez, E., & Ramsey, A. (2014). Danger, danger! Evaluating the accessibility of Web-based emergency alert sign-ups in the northeastern United States. *Government Information Quarterly*, *31*(3), 488-497.

Wireless RERC. (2016). *Observations of the 2016 National EAS Test*. Retrieved from http://cacp.gatech.edu/sites/default/files/docs/Research%20Brief%20Observations%20of%20the%202016%20National%20EAS%20Test.pdf

Wirth, A. (2017). Cyberinsights: It's time for belts and suspenders. *Biomedical Instrumentation & Technology*, *51*(4), 341-345.

WKTV. (2016). WKTV scrolling message alert. Retrieved from https://archive.fo/DT8kE#selection-1495.0-1514.0

Wrona, K., Moye, T., Lagadec, P., Street, M., Lenk, P., & Jordan, F. (2018). Cybersecurity innovation in NATO: Lessons learned and recommendations. *Information & Security*, *36*, 1-25.

Xu, K., Liao, Y., Qiao, L., Liu, Z., & Yang, X. (2015). An identity-based (IDB) broadcast encryption scheme with personalized messages. *PLoS One*, *10*(12), 1-11.

Zeichner, L. M. (2001). Developing an overarching legal framework for critical service delivery in America's cities: Three recommendations for enhancing security and reliability. *Government Information Quarterly*, *18*(4), 279-291.

About the Authors

Andrew Green is a Lecturer of Information Security and Assurance in the Information Systems Department, located in the Michael J. Coles College of Business at Kennesaw State University, Kennesaw Georgia. He earned his Bachelor of Science in Information Systems from Kennesaw State University, his Master of Science in Information Systems from Kennesaw State University, and is currently completing his PhD at Nova Southeastern University. He researches at the intersection of information security, privacy, and public policy and has published on this and other topics at numerous conferences and in *Journal of Information Systems Education*. He has also co-authored several academic textbooks in the information security arena. He has almost two decades of industry experience in information security. Before entering academia full-time, he worked as an information security consultant, focusing primarily on the needs of small and medium-sized businesses.

Amy B. Woszczynski is Professor of Information Systems in the Michael J. Coles College of Business at Kennesaw State University. She earned a Bachelor's in Industrial Engineering from Georgia Tech, an MBA from Kennesaw State University, and a PhD from Clemson University. She researches on social, culture, and diversity issues related to information technology, information security policies, and information systems/information security education. She has published on these and other topics in journals such as *Computers in Human Behavior*, *Journal of Global Information Technology Management*, *Journal of Computer Information Systems*, *Industrial Management & Data Systems, Journal of Information Systems Education*, and *International Journal of Information Management*. She co-edited *The Handbook of Information Systems Research* and *Handbook of Distance Learning for Real-Time and Asynchronous Information Technology Education*.

Kelly Dodson is a 2018 graduate of the Michael J. Coles College of Business, Kennesaw State University. She earned her Bachelor of Business Administration degree in Information Security and Assurance. In 2018, she was selected as the “ISA Student of the Year” by department faculty, in recognition of her outstanding academic performance. After graduation, she took a position as an Information Security consultant with a large accounting and auditing firm, based in the Atlanta area.

Peter Easton is a 2018 graduate of the Michael J. Coles College of Business, Kennesaw State University. He earned his Bachelor of Business Administration degree in Information Security and Assurance. After graduation, he took a position as an infrastructure engineer with a large defense contractor, based in the Washington, DC, area.