2019

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

Andrew Green, *Kennesaw State University*
Amy B. Woszczynski

Communications of the
Association for Information Systems

Accepted Manuscript

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

Communications of the Association for Information Systems

Research Paper 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:

U.S. emergency alert systems (EASs) are part of the nation's critical infrastructure. These systems are built on aging platforms and suffer from a fragmented interconnected network of partnerships. Some EASs have an easily identifiable vulnerability - their management website is available via the Internet. Authorities must secure these systems quickly. Other concerns exist, primarily the lack of policies for reporting vulnerabilities. To begin an assessment of U.S. EASs, we used Shodan to evaluate the availability of these websites in six southeastern states. We found 18 such websites that were accessible via the Internet, only requiring user credentials to login to the system. Next, we searched for published policies on the reporting of vulnerabilities; we found no vulnerability disclosure policies for any of the systems 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, along with system resilience, as lines of defense against cybersecurity threats. By implementing these strategies, U.S. EASs will be positioned to update critical infrastructure, notify groups of emergencies, and ensure the distribution of valid and reliable information to the populations at risk.

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

1 Introduction

In 2013, numerous emergency alert systems (EASs) in Michigan, Montana, and New Mexico found themselves in the middle of the zombie apocalypse, when the following alert was improperly sent (Paul, 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."*

The systems exploited in the zombie hoax were vulnerable due to default passwords that were not changed upon receipt of hardware, allowing cybercriminals to access the insecure systems and distribute a message of their choice to the population. The initial passwords were publicly available on the Internet, along with other operating instructions from Digital Alert Systems/Monroe Electronics (DAS/ME), a leading provider of hardware 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 of unauthorized access by cybercriminals. 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.

Are U.S. EASs vulnerable to attack? If so, is the network of EAS providers aware of the vulnerabilities in these systems, and are they working to establish effective, efficient, and consistent cybersecurity standards? The evidence available tends to show that U.S. EASs, as part of the nation's critical infrastructure, are under-protected (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 were still using default passwords, months after his original alert to the vendors (Ollmann, 2013).

More recently, Hawaii's EAS experienced a very public and embarrassing incident, caused by human error, when a wrong button was pressed (Kang, 2018). The SMS message, which was sent to all Hawaii residents, read: "BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL" (Sagan, 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. More concerning, however, is that outsiders were able to take control of the systems and send – or not send – messages of their choice.

EASs should be secure while distributing valid and reliable information to the relevant population in an effective and timely manner. Past performance does not lead to confidence in U.S. EASs. This paper proposes the use of technical guidelines, as well as management strategies, to plan and prepare for vulnerabilities found in fragmented, decentralized EASs. Sadly, some EAS providers are not following technical guidelines or using management strategies to secure their networks, thus increasing opportunities for cybercriminals to compromise systems. Part of the problem is a lack of 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 of overcoming inevitable failures, but the lack of funding limits opportunities to protect EASs.

Previous academic work has not evaluated the security of the EASs or countermeasures that could be taken 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 2-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 regarding the reporting of vulnerabilities. We provide a set of 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. First, we examine the current state of the EASs in the U.S., as described in the next section.

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

2.1 EAS overview

In the U.S., the EAS is a national public warning system used by individual television, radio, cable, and satellite broadcasters to deliver emergency alerts to the public (Federal Communications Commission, 2018). The primary purpose of the EAS is to allow affected people to receive critical, timely, and relevant information regarding an emergency. At the national level, the President may call for an announcement to the public regarding a national emergency; more commonly, state and local authorities use the decentralized architecture of the EAS 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, an EAS message is formatted using the proper protocol and is transmitted via a daisy-chain style distribution method from broadcaster to broadcaster, until the message is fully distributed (Federal Communications Commission, 2018). In the second method, EAS messages are delivered via the Internet through the Integrated Public Alert and Warning System (IPAWS), a system administered by the Federal Emergency Management Agency (FEMA) (Federal Communications Commission, 2018). In this study, we examine vulnerabilities present in decentralized EASs at the individual broadcaster level, and not on the IPAWS.

2.2 Definitions

Throughout this paper, we will use the following terms:

- Emergency Alert System (EAS) – A public warning system that requires broadcasters to provide communications capabilities to the President, state, and local authorities, to address the affected population during an emergency (Federal Communications Commission, n.d.).
- Internet-facing EAS management website – A website which provides administrative access to an individual broadcaster’s EAS infrastructure. This website is accessible via the Internet with nothing other than a web browser; users authenticate by way of 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 signals received 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); the EAS managers at the local, state, and regional levels; and the population receiving the emergency warning alerts.

2.3 History of EAS Vulnerabilities

As shown in Table 1, EAS vulnerabilities are not new. 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 easy access to information, quickly and efficiently. Curious people chanced upon vulnerable systems, while malicious actors began to capitalize on system vulnerabilities. Once vulnerable systems were identified, individuals began sharing information with a widely dispersed and Internet-connected population. Mistakes were made, and – in some cases – the public became aware of the errors.

Meanwhile, Michigan, Montana, and New Mexico received devastating news in 2013 – the zombie apocalypse was here! (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 were able to login with details found there. In addition to the default credentials being available on the Internet, the EAS management websites were accessible via the Internet (Reuters, 2013). Several months after the zombie hoax, the number of vulnerable systems increased (Paul, 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% 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 September 28, 2016, cybercriminals compromised the EAS at WKTV, a TV station in Utica, New York, and broadcast 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 April 7, 2017, Dallas residents awoke to sirens in the middle of the night; authorities were unable to deactivate the sirens for 90 minutes (Hub, 2017). In the Dallas case, the system was accessed using radio frequencies and may not have been encrypted, making it more vulnerable to threats (McFarlane, 2017). Almost a year later, in early 2018, Hawaii made news, warning its 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 vulnerable systems, and to resolve them, ensuring the corrections are issued immediately when a false alert is sent (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 June 26, 2007, Illinois state officials distributed an Emergency Action Notification (EAN), a direct message from the President of the United States (FEMA Fact Sheet, 2007). In the 2007 incident, a local contractor accidentally left a satellite distribution receiver in the "on" mode, and the message was sent 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; the failure rate of systems receiving the message was about 18% (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; AT&T U-verse viewers were not allowed to change the channel and were told 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 because of 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% of television tests included the slide, text crawl and audio components that were required for a fully successful test; further, they noted several issues that needed to be addressed to improve access to those with disabilities and to those who speak languages other than English. States responded to these deficiencies, offering sign-up sheets for persons with disabilities. However, they were still unable to reach the targeted group, with over 80% of counties reporting accessibility violations (Wentz, et al., 2014).

More recently, in October 2018, government authorities conducted the first test of the EAN on mobile phones. 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 were unable to 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 most alerts are issued at the local and/or state levels, a focus on vulnerability at the national level is insufficient to ensure capabilities of the EASs. Are these systems vulnerable to cyberattack?

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 of reliable data every single time ensures that people understand that the information is valid, relevant, timely, and real-world. If there are 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, EASs are vulnerable, and cybercriminals could have a "field day with the Emergency Alert System" (Albanesius, 2013). Wimberly (2014) concurs, noting that EASs need "serious attention," while Dodril (2016) argues that EASs are as vulnerable to attack as other national infrastructures; she goes on to warn of the potential impact if cybercriminals compromise EASs. John Hickenlooper, Governor of Colorado, voiced concerns about the security of EASs, 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 that were initially developed in the 1980s (McFarlane, 2017), it is clear that EASs are vulnerable to access by cybercriminals (Constantin, 2013). Even when EASs are not directly connected to the Internet with open access, authorities have to worry about vulnerabilities in the equipment that is used to transmit the alerts (Albanesius, 2013). In some cases, EASs remain vulnerable because of a lack of preparation and awareness of the cybersecurity issues that exist (Hub, 2017). Resolving the problem is not easy.

While the recent cyberattacks on EASs demonstrated how attackers used vulnerabilities with little community impact, a much more severe scenario is 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, road closings could be broadcast using the EAS, directing residents to a particular route, which is then attacked. While these cyberterrorist attacks have not yet occurred, the vulnerability of the EAS remains a serious concern, particularly with 85% of critical infrastructures being locally or privately owned (Egli, 2013); thus, system vulnerability at the local, most decentralized level, is essential. With cybercriminals working together, sometimes at the direction of nations in opposition to the U.S., state and local EASs may find it quite challenging to mount a sustained defense (Claus, Gandhi, Rawnsley, & Crowe, 2015). At the local levels, which receive less funding and have less cybersecurity expertise, the risk is even more significant than the national level (McFarlane, 2017).

Further complicating protection of the EASs, disaster management is often viewed in a silo manner, considering each level in the chain without planning for the interconnected network (Egli, 2013). Without coordination throughout all levels of EASs, local levels will likely continue to face the problem of 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, thus reducing system vulnerability (Li, 2015).

Contemporary technology developments emphasize the importance of each link in the system, no matter how small or large the link is. Each link in the partnership must be prepared to address continued cybersecurity challenges. For instance, the rise of the Internet of Things has dramatically increased the number of connections that must be secured, using devices owned individually, by private organizations, and by the government. These connections, along with the need for remote access to critical systems, increase the vulnerability of EASs to unauthorized access (McFarlane, 2017; Meshkati & Tabibzadeh, 2016). While it is difficult to secure all of the connections throughout the EAS supply chain (Morrison, 2013), authorities 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 EAS vulnerabilities, organizations need to have a trained and aware staff; security education, training, and awareness (SETA) policies should be emphasized at all levels. However, local governments face continued underfunding of SETA opportunities. Meshkati & Tabibzadeh (2016) found that EAS authorities often believe that their personnel are not adequately trained in security and information protections; in fact, just over 70% of local governments reported that lack of end-user training was a modest or severe barrier to cybersecurity efforts. Without sufficient training of those who use the system, cybersecurity protections may be less effective. Moreover, as long as cybercriminals continue to believe that local systems are vulnerable and that they likely will not be caught, they will continue to search for and penetrate these access points (Metivier, 2017). Compounding the issue of system vulnerability is the ongoing struggle to hire qualified, well-trained cybersecurity experts to work with the EASs, at substantially lower government wages as compared to their peers in the private sector (Nixon, 2016). The attacks on points in the critical infrastructure of the EAS continue unabated, highlighting the need for a clear, unambiguous, coordinated method of securing vulnerable systems throughout the EAS network. The next section outlines steps that the EAS network may take to reduce vulnerabilities.

3 Steps to Reduce Vulnerabilities

Developing a risk management plan that brings together all of the partners in the EAS supply chain is challenging to implement, monitor, and manage. With current cybersecurity policies and practices that are fragmented and non-cumulative across all the partners in the supply chain of critical infrastructure, an over-arching, integrated risk management approach is essential (DiMase, Collier, & Linkov, 2015). Partners in the EAS supply chain have diverse backgrounds that complicate efforts to work together, presenting cybersecurity professionals with 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, as well as media, who have a more liberal arts education, and the public, with diverse backgrounds, which likely will not be known in advance. The difficulty in communicating with these diverse partners is only complicated when technology partners enter the picture. This diversity of 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 the implementation of risk management plans, it does allow the opportunity to build upon local and traditional knowledge and strategies to better understand the complex network of EASs (Baudoin, Henly-Shepard, Fernando, Sitati, & Zommers, 2016). Closer coordination between all entities, no matter their backgrounds, is necessary to properly manage cybersecurity (Borchert, 2015). Further, technical shutdown procedures must be developed and implemented as part of the overall risk management plan, and a backup system should be available 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 within the group, deploying management practices in response, and then developing technical controls to reduce vulnerabilities.

Cybersecurity professionals developing risk management plans for EAS authorities should have a clear understanding of infrastructure dependencies, including the public-private-government partnerships present in most EASs, and should be able to determine the cascading damages that may result from attacks (Zeichner, 2001). Technical expertise in the field is essential to understanding the potential impact of cyberattacks. Cybersecurity risk management plans are incentivized to minimize risk, particularly at the national level, which is highly regulated; by contrast, cities, counties, and localities face fewer regulatory requirements (McFarlane, 2017), opening 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 are burdensome and expensive. Recently, 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). This step was taken 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 to the exclusion of other partners (Egli, 2013), risk management policies should consider all partners in the public-private-government chain, as well as the distributors and receivers of information, such as the public at large, forecasters, media liaisons, and the like. A deep understanding of the partners leads to awareness of relevant social structures and how to integrate management and technical best practices into the design, development, and ongoing maintenance of 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 the inevitable cybersecurity breach occurs, a good risk management plan will help ensure that the network is resilient (Jung & Song, 2015) and able to respond to the threat. Cybersecurity professionals must work with EAS authorities to develop a risk management plan while educating those in the network on how to minimize threats to the EAS supply chain.

Throughout this section, we have discussed the complexities in responding to cybersecurity challenges. Cybersecurity professionals must not rely on technical expertise alone. Instead, they must have a keen awareness of social dynamics and how people will use the system in unintended ways, developing managerial policies accounting for social dynamics. Technical skills without an understanding of social skills (or vice versa) will not lead to ideal outcomes. In the next section, we examine steps to reduce vulnerabilities, dividing them into issues that are predominantly technical or social, while realizing that there is often overlap in the two areas. We begin with technical cybersecurity issues, which include prioritizing threats, using appropriate encryption, and testing systems.

3.1 Technical Issues

3.1.1 Prioritization of Threats

All threats are not equal. Some threats, though unlikely to occur, could present devastating and cascading effects on EASs. Other threats, while likely, may present less potential damage if the vulnerability is exploited. Cybersecurity professionals must prioritize threats and provide protections in line with the likelihood and severity of the threat. Borchert (2015) asserts that organizations should prioritize and manage threats that are "core issues" (serious, short term technical threats), as well as "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. Those threats which may interfere with the ability of EASs to deliver information to the right people at the right time and in the right format should be addressed first, as a core issue, with a descending order of priority. Aging infrastructure, which, over the long term, may affect the performance of all systems on the interconnected network, are considered a cross-cutting issue and should be addressed in long-term planning. Cybersecurity professionals should stay abreast of current developments that may present a threat to EASs, including the use of social media to identify, prioritize, and respond to threats (Sheffi, 2015). EAS authorities should periodically re-evaluate threats, however, since those that are currently a long-term threat may become a core issue if not addressed promptly. In addition to prioritizing threats, there are several other steps to protect the data and information in the EAS network, including encryption of data and regular systems testing, as described in the next sections.

3.1.2 Use of Encryption

Researchers widely agree that there is a need for encryption when sending EAS messages (Loukas, Gan, & Tuan, 2013; Seddigh, Nandy, & Lambadaris, 2006; Shu, Lee, & Yannakakis, 2006). In the Dallas siren example discussed previously, the cybercriminals accessed the system through unencrypted radio signals (Hub, 2017); strong encryption may have prevented that cyberattack from taking place. Populations receiving EAS messages are transient, changing often and perhaps in unexpected manners. From a public policy and safety perspective, when an emergency happens, there is no real difference between a citizen of a region and someone who is visiting temporarily or just passing through the area – everyone in the affected region needs to receive an EAS message when it is sent. Schulzrinne and Arabshian (2002) proposed a method of allowing user devices to auto-subscribe to alerts based on their geographical proximity. However, this proposed method was silent on the matter of message encryption. 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 within 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, previously unknown to each other, to establish an encryption key to allow for secure transmission of data from sender to 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 a number of 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 addressing the issues surrounding secure messages being sent by a verified and trusted source. However, the underlying requirements for the scheme to work, such as smart cards or pre-distributed encryption keys, make the system impractical for use in the delivery of EAS messages. As Shu et al. (2006) noted, broadcast encryption is well suited for use in pay television programming and Internet-based software distribution but poses implementation challenges in EASs.

As we have demonstrated, the use of encryption in EAS message dissemination is complex, with a wide array of concerns and obvious technology limitations. Possible solutions to address these concerns are outside the scope of this research paper, and frankly, outside the scope of current practical technology capabilities. As technology continues to evolve and as impediments to encryption are resolved, future researchers should investigate methods of addressing this issue. We feel strongly that these issues must continue to be explored in order to protect the critical infrastructure of EASs in the U.S. While encryption capabilities are limited, organizations working with EASs should encrypt as much as possible, responsibly and proactively, and through regular systems testing, as described in the next section.

3.1.3 Regular System Tests

Local EAS officials should perform regular testing (Wimberly, 2014) and create backups of 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 an organization's vulnerabilities are viewable with a simple Google search, systems testing is not thorough.

Further, software should be properly maintained, updated and patched over time (Wirth, 2017), with a 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 is challenging to accomplish, since few EAS authorities have funding to complete a thorough evaluation of systems (Borchert, 2015).

Organizations that prioritize threats, use appropriate encryption, and regularly test systems are likely to be ready for cybersecurity challenges, at least from a technical perspective. However, the most technically capable system may fail if social complexities are not recognized. Now, we move to a discussion of the social realities of an extensive, fragmented public-private-government interconnected network of systems. As funding continues to be tight, EAS authorities may have to find unique methods of engaging with users, cybersecurity professionals, and EAS hardware and software providers, to help identify vulnerable systems. As we discuss in further detail below, coordinated vulnerability disclosure (CVD) policies should be established as part of an overall plan to involve diverse stakeholders in securing EASs nationwide, in order to identify vulnerable systems as soon as possible.

3.2 Social Issues and Managerial Challenges

3.2.1 Establishment of Coordinated Vulnerability Disclosure (CVD) Policies

It is unrealistic and naïve to assume that EAS authorities can eliminate all vulnerabilities. However, there are several steps that EAS authorities may take to improve security. One step is to ensure that vulnerabilities, when found, may be quickly reported to the appropriate authority for resolution. While those who report vulnerabilities may be individuals, McFarlane (2017) recommends that crowdsourcing should not be overlooked as a valid option, using groups of cybersecurity researchers to identify threats as a supplement to IT staff working for cash-strapped EAS entities. However, in 2015, of Forbes Global 2000 companies, only 6% had a method for external cybersecurity researchers to identify, describe, and report a vulnerability (Branscombe, 2017). Thus, cybersecurity researchers may not know whom to contact regarding the vulnerability. As a result, efforts to identify vulnerabilities revert to the local, state, federal, and non-government agencies who are involved in managing the U.S. EASs. The current approach is fragmented (DiMase, Collier, & Linkov, 2015); this non-standardized, non-cumulative approach to managing vulnerabilities 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 which 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 are capable of identifying vulnerabilities and alerting the organization in a coordinated and secure manner. The CVD policy must be clear, however, or cybersecurity researchers will be hesitant to participate. Claus, Gandhi, Rawnsley, & Crowe (2015) note the importance of assuring that vulnerability information submitted will be kept confidential, in order to establish trust between EAS authorities and those who might report vulnerabilities. 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, which currently comprise the U.S. EAS, the added complexity may be worth the potential value gained.

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 should be evaluated. Borchert (2015) asserts that corporate security and national security are intertwined. As cloud computing and other distributed systems continue to proliferate, it is incumbent upon governmental agencies at the federal, state, and local levels to seek partnerships with companies who view cybersecurity as a strategic priority. Moreover, critical cybersecurity recommendations require that government agencies share cyber threat data, guidelines, and best practices (Claus, Gandhi, Rawnsley, & Crowe, 2015; Rodin, 2015), and we recommend extending these governance guidelines to all partners in the public-private-government network of EAS providers. 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). A deep understanding of how technology in the network interacts with and is interoperable with, other elements in the partnership, is essential to establishing cybersecurity safeguards (Meshkati & Tabibzadeh, 2016).

The U.S. EAS is complex, with numerous elements in its supply chain, countless vendors, and a lack of consistent cybersecurity standards. In such a situation, securing critical infrastructure at all points in the network is difficult (Morrison, 2013). While many have recommended public-private-government partnerships to improve the security of critical infrastructures, including the U.S. EAS (Borchert, 2015; Claus, Gandhi, Rawnsley, & Crowe, 2015; Eichensehr, 2017; Manley, 2015; Marett, 2015), there has been little practical implementation or testing of such partnerships. Cybersecurity becomes more difficult in these highly complex, interconnected networks. Government agencies with critical infrastructure interests, such as EASs, must evaluate all members of the network – and use the evaluation as a part of the selection process when new vendors are chosen; 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 used for U.S. EASs, each partner is only as reliable as the weakest connection in the chain. Cybercriminals will look to illegally access the weakest partner, gaining a foothold from which to pivot their attack against other partners, in order to achieve their objectives on targets like EASs. These interconnected networks of widely dispersed partners, with varying and sometimes competing goals (Eichensehr, 2017) add to the vulnerability of the systems. 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. The best plans, however, are not made at a high-level with little consultation with partners in the chain; instead, soliciting feedback and recommendations from users in the EAS network is recommended.

3.2.3 Direct Involvement of Citizens

EAS stakeholders are a diverse group, with different perspectives and understanding of how the system should function. From the government perspective, officials responsible for emergency management and response, at the federal, state and local levels, qualify as stakeholders. Publicly broadcast television and radio stations also qualify as stakeholders, as do cellular telephone providers. This rich, diverse group possesses varying levels of knowledge, relative to their place in the EAS ecosystem. Stakeholders at the national level of the EAS will have different perspectives than their state and local counterparts. Bringing together stakeholders at different levels may lead to a better understanding of potential vulnerabilities. Directly involving stakeholders who possess large amounts of local knowledge, allows the development of community-centric networks (Baudoin, Henly-Shepard, Fernando, Sitati, & Zommers, 2016). Stakeholders in these community-centric networks can learn from each other and strengthen the EAS through sharing knowledge within, between, and among users at different levels of the public-private-government partnership. If EAS authorities develop CVDs as described previously, the network expands to include cybersecurity researchers, who, with EAS managers, can synergistically work together to improve the security of vulnerable systems over time. Citizens who are familiar with technology should also be drafted to distribute the word when an emergency occurs. For instance, by enlisting citizens to spread the word on Twitter during a recent tsunami, a large number of people were informed quickly and efficiently, through tweets and re-tweets of relevant information (Chatfield, Scholl, & Brajawidagda, 2013). Similarly, other social media platforms should be used to stay up-to-date on potential security vulnerabilities, allowing EAS authorities 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 the use of Twitter was an overall benefit during the disaster, governments should plan in advance for citizen involvement, 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 is a matter of public safety; they must provide reliable, accurate, updated, and timely information to the population at risk. Complicating matters, EASs are jointly managed by numerous agencies at the federal level, including 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, it is clear that 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, it is challenging to 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, Collier, & Linkov, 2015; Egli, 2013; Karlsson, Kolkowska, & Prenkert, 2016; Peeters, 2017; Jung & Song, 2015). U.S. Cyber Strategy agrees, calling for cyber resilience strategies and sustainable networks when an attack occurs for any of the branches 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 network of EAS providers will not reduce all threats. When a system is resilient, it does, however, reduce the impact of threats on the system as a whole, as well as the cascading threats throughout the network (Tagarev, Sharkov, & Stoianov, 2017).

Complicating the matter, resilience is not easy to define, 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 resilience of the network at large is somewhat fragmented and non-cumulative (DiMase, Collier, & Linkov, 2015; Egli, 2013; Meshkati & Tabibzadeh, 2016), with a lack of understanding of the complex cybersecurity issues that arise throughout the interconnected enterprises (DiMase, Collier, & Linkov, 2015). With many such public-private-government connections throughout the critical infrastructure of the EAS, resilience is often defined by different groups, 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, with specified roles and responsibilities, to protect, defend, and recover EASs (Raab, Jones, & Székely, 2015) and with the ability to communicate emergency information and alerts to populations at the federal, state, and local levels. Building on the interconnected nature of EASs, Egli goes further, viewing resilience "as a public good enabled by collective action, interagency coordination, and public-private partnerships" (2013, p. 32). Wrona et al. (2018) concur with the idea of resilience, advocating for a "Fail Fast" option, where organizations embrace failures and learn from them, improving security and resilience over time. However, some authors have cautioned organizations not to fall into the cybersecurity paradox, where the infrastructure is strengthened at the expense of individual privacy rights, and instead, recommend securing the organization and building resilience while ensuring that individual privacy is protected (Dunn-Cavelty, 2014; Raab, Jones, & Székely, 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 within the integrated and interconnected system (Meshkati & Tabibzadeh, 2016).

Moreover, since most EASs are owned and operated privately (Borchert, 2015; Egli, 2013), they tend to focus on their own immediate needs and may not consider the importance of interconnectivity. However, this ability to connect is essential, 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% of the US population lives in 11 mega-regions (Todorovich, 2008), a well-positioned interconnected network that is resilient in the face of disaster, could serve a large portion of the U.S. 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 cybersecurity challenge to the U.S. EAS is daunting; reducing system vulnerabilities across every region, state, city, county, and municipality is difficult. There is no easy fix, and vulnerabilities may vary from location to location. However, to evaluate the cybersecurity challenges facing U.S. EASs, we completed a review of the current open availability of EASs, along with current vulnerability disclosure policies, of the southeastern region of the U.S. Our method provides a first look at U.S. EASs, as described in the next section.

4 Method

We searched for Internet-accessible EAS management websites from six southeastern states, to determine whether any were available via either HTTP or HTTPS. To do this, we used the Shodan application (https://www.shodan.io/). Shodan is a publicly available application which indexes search results for websites, networked devices and the like, with details pertinent to security researchers (Barnaghi & Sheth, 2016; Konstantinou, Sazos, & Maniatakos, 2016; Serbanescu, Obermeier, & Yu, 2015). Using data from the Shodan application is not without concerns, however. As Konstantinou, et al. (2016) noted, there is some question as to how frequently the Shodan application scans the Internet for new data, as well as how often those results are indexed 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 DAS/ME, we were able to locate EAS technology products made by Everbridge, Inspiron Logistics, and Vesta Public Safety (formerly known as Cassidian Communications).

However, none of these websites had enough detail to allow us to determine which municipality was using them, thus preventing further analysis. The DAS/ME instances, however, did provide us with enough detail to gather and analyze the data. Since DAS/ME has been reported 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. While Shodan yielded many websites, indicating potential Internet-accessible EAS management websites, the number was incomplete for our analysis. After identification, we further evaluated each instance before including in our study. First, we visited each of the URLs identified and determined if the website met our specific definition as an Internet-accessible EAS management interface website. During this process, also eliminated duplicate instances; e.g., where a specific municipality had already been included in our results. In some cases, 20 or more instances returned by Shodan were ultimately identified as belonging to only one EAS system. Nevertheless, each instance had to be carefully checked and analyzed for inclusion 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 did a deeper dive to search 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 needed for each Shodan instance, 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, including IP address, TLS encryption details (when encryption was enabled), and city name associated with the IP address. We then aggregated the search results into a spreadsheet for further analysis.

Next, we manually visited each of the EAS management websites listed in the Shodan output, using a web browser. During this phase, we collected additional data. In particular, data collected included displayed website name, municipality name when displayed, EAS serial number and platform ID, analog and digital transmitter details, as well as the date/time the student researchers accessed the website. It is important to note that all of this data was available from the EAS management website's login page, with no additional steps taken other than to visit the IP address using a web browser. No further reconnaissance was conducted against any of the EAS management websites visited, outside of the Shodan results collected and the manual viewing of 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 visited. 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 visited. We all agreed that we would not attempt any type of login on any of the EAS management websites examined, as we were not authorized to do so by the respective system owners.

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 are potential targets for brute-force attacks, wherein cybercriminals try various combinations of usernames and passwords to gain unauthorized access. Once cybercriminals gain access to an EAS management website, they could choose from a variety of actions, including: changing basic system configuration options like radio frequencies used to broadcast messages; triggering warning sirens; sending fake alerts; canceling existing valid alerts; or disrupting the ability to send alerts completely. Such actions could mean the difference between life and death of the people in the geographic area of interest; thus, those cybersecurity professionals designing, maintaining, and securing EASs must be very confident that the systems will work as intended. Loss of life due to a compromised system is not acceptable. Our analysis yielded 18 Internet-accessible EAS management websites across the southeastern United States, as shown in Table 2.

Table 2. States and Number of Internet-accessible EAS management websites

State	# 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

If a cybersecurity researcher identifies vulnerabilities, what is the next step? Perhaps the vulnerability could be reported to EAS authorities following published vulnerability disclosure guidelines? Unfortunately, none of the 18 Internet-accessible EAS management websites had a process in place to report the vulnerability. We intended to inform the appropriate EAS authorities of the vulnerabilities in their respective systems; but there was no public method that we, as cybersecurity researchers, could undertake to inform the appropriate EAS authorities.

The focus on vulnerability disclosure policies has historically been by way of application developers and having a process by which cybersecurity researchers can inform them of vulnerabilities found in their products. However, all organizations face vulnerabilities and their associated risks, not just application developers; similarly, vulnerabilities may be discovered by anyone, not just cybersecurity researchers.

Our research into EAS management websites highlights a vulnerability that exists not because of a flaw in an application, but because of how an organization chose to implement an application in their network. For instance, EAS providers ignored the specific advice from DAS/ME and did not change the admin password when the system was installed. 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, irrespective 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 if found.

6 Analysis of Results

6.1 Internet-accessible EAS management websites

Of the six states we investigated, all of them had at least one Internet-accessible EAS management website interface. Multiple websites offered access using HTTP, which is especially troubling because traffic sent via HTTP is unencrypted and can be read by anyone capable of capturing that network traffic. 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 open website. For an essential component of the U.S. national infrastructure, we contend that not one Internet-accessible EAS management website should be openly available, requiring a simple user id and password to authenticate and access management capabilities for the EASs.

Within the six states analyzed, there is at least one weak link in each. 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. Regular systems testing, along with the use of Shodan or other Internet-scanning applications, can ensure that EAS owners do not overlook vulnerabilities. Systems testing should also include verifying no default passwords are in use.

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 members of the EAS network, implementing more electronic filing of EAS risk management plans, much like the ARS recently implemented (RadioResource, 2018). EAS authorities at all levels should seek ways of reducing burdensome requirements, allowing those in the supply chain to focus on cybersecurity initiatives to strengthen the system as a whole. While the ARS is a step in the right direction, other opportunities should be investigated as well.

Since funding is likely to continue to be in short supply, we encourage EAS authorities to consider using the network of highly trained cybersecurity professionals to help them find vulnerabilities. EAS authorities should also closely monitor social media and the cybersecurity community. If users note concerns with receiving messages from the EAS authorities, for instance, they will likely post on social media, allowing another cybersecurity analysis from the user perspective. Also, EAS authorities should monitor cybersecurity forums for evidence that system vulnerabilities are present. Our paper highlights the importance of technical and social skills, along with the implementation of appropriate management policies, for those who lead the cybersecurity efforts in the EAS network.

6.2 Vulnerability Disclosure Policies

Assuming that someone found a vulnerability, what are their options? As cybersecurity researchers, we wanted to disclose the vulnerabilities we identified in each state. Since none of the entities with the Internet-accessible EAS management websites had a published method of reporting the vulnerability, there was no clear process for us to follow in our attempts to report the cybersecurity concerns. Moving to a higher level, we also examined the state EAS websites, which, at the time of this writing, offered no path to report vulnerabilities. Thus, it is unsurprising that other entities, lower in the EAS supply chain, failed to provide a method of reporting vulnerabilities. We encourage the network of EAS providers to publish a vulnerability disclosure process. At the least, it offers free cybersecurity help; at the most, the process may encourage testing beyond what each entity is capable of undertaking, given inadequate funding.

The network of cybersecurity professionals is 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 are unable to report directly to the affected portion of the EAS supply chain. Instead, the researcher may abandon the vulnerability. Alternatively, the cybersecurity researcher may report it publicly, hoping to incentivize the system owners to address the vulnerability. Unfortunately, the uncoordinated disclosure of the vulnerability may make the system even less secure until a mitigation strategy is developed. However, if local, city, county, state, and federal emergency management authorities publish a way to report the vulnerability, the problem could be resolved quietly, and then a coordinated disclosure – after the vulnerability is mitigated – could give the researcher credit for the discovery, and allow the critical infrastructure in the U.S. to continuously improve.

EAS authorities must publish a way for cybersecurity researchers to report vulnerabilities without fear of reprisal. While we recommend the creation of CVD policies, any easy to find vulnerability policy would be better than what is available now. We further recommend that the policy explicitly absolves anyone who reports the vulnerability, of any legal or civil penalties – as long as the vulnerability is only located and disclosed as specified in the policy, and not attacked. Since the network is comprised of numerous public, private, and governmental owners of EAS assets, there must be coordination among and between the groups, when developing a policy on vulnerability disclosure – up, down, and across the supply chain. Otherwise, cybercriminals are likely to exploit any discovered vulnerabilities, potentially compromising the entire EAS network.

We will not identify the Internet-accessible EAS management websites that we discovered. Some of the websites we discovered may have been removed from the Internet during our research, while new websites may have been put online and made Internet-accessible. We strongly encourage all EAS authorities to provide a proper method of reporting identified vulnerabilities. Cybersecurity researchers want to help; please allow us to do so.

6.3 Restricting access to EAS management websites

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

To mitigate this risk, we propose a multi-step technical solution for EAS owners. First, we propose placement of the EAS management website on the organization's internal network, thus removing it from direct Internet access. Next, we propose the website be placed on a virtual local area network (VLAN) segment within the organization's internal network, to further restrict access to the EAS management website to specific IP addresses within the internal network. VLANs are a common networking control used 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 the EAS can be accessed remotely if needed, as recommended in NIST special publication 800-77 (Frankel et al., 2005). We propose restricting VPN access to defined VLANs, and limiting access based on authorization to use the EAS management website, including individuals who are authorized to 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, VPN user authentication could be configured to deny access from non-US based IP addresses, also known as geolocation (Taylor, Devlin, & Curran, 2012). We concede that user authentication is of limited effectiveness due to the relative ease and availability of proxy servers with US-based IP addresses (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. EAS default admin passwords are sometimes available in system documentation on the EAS manufacturer's website, which is easily accessible to anyone who does a quick Google search. 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, thus removing the possibility of ever attaching it directly to the Internet.

6.4 Overall Recommendations

Throughout the EAS network, threats should be prioritized, with a consistent set of policies that seeks to maximize the security of the entire EAS network, rather than allowing each EAS authority to create and use individually developed, decentralized, and fragmented plans. Regularly testing EASs in a structured and standardized manner is also recommended, and would help to avoid the reuse of default passwords, for instance; continuous system testing is recommended to ensure high levels of cybersecurity preparedness. To accomplish these technical goals, relationships between and among partners in the EAS supply chain should be cultivated, with the goal of improved security for EASs, and with the direct involvement of citizens, who are most impacted by emergency alerts in local areas. Since we realize that vulnerabilities are impossible to prevent, even with proper planning, we recommend that members of the EAS supply chain publish a set of vulnerability disclosure policies, allowing for their use by cybersecurity professionals, who may find potential problems and want to report them. For EAS providers who fail to follow technical guidelines and managerial strategies, an insecure network and cybercriminals are likely to compromise the network. While most known attacks on EASs have not resulted in problems with the distribution of valid warnings, the future is 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 those who are authorized to use the decentralized systems. With cybercriminals from other countries attempting to infiltrate elections systems, email servers, and the like, it is reasonable to assume that cybercriminals have tried – and will keep trying – to infiltrate EASs as a method of disrupting one of the critical infrastructure systems for the U.S.

7 Limitations and Future Research

Our study is not without limitations. Additional generation and testing of theoretical foundations of potential vulnerabilities in U.S. EASs is an important avenue of future research. We described methods to improve resilience and increase the security of only one particular critical infrastructure system – the EAS, providing a specific context. Future researchers will no doubt find it challenging to test the resilience and vulnerability of EASs because of the secrecy shrouding critical governmental infrastructure (Karlsson, Kolkowska, & Prenkert, 2016). Also, while we recommended encryption of EAS data, there is no good solution currently available to encrypt data at rest and in motion; 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 be externally generalizable to EASs outside of the U.S., since other countries may have specific contextual factors that differ from the U.S. EASs discussed here (Ochara, 2017). Similarly, other regions of the country may have different characteristics than the southeastern U.S. that we examined. Another limitation of our research is the decision to examine systems from DAS/ME. We were able to identify Internet-accessible EAS management websites for products made by other providers; however, beyond DAS/ME, none of these websites had enough detail to allow us to determine which municipality was using them, thus preventing further analysis. As a result, we only included DAS/ME for our analysis. However, DAS/ME is a leader in EASs and is mentioned often in news reviews; thus, we believe that the selection of DAS/ME was practical, relevant, and appropriate.

While we made several recommendations to secure vulnerable EASs, other technical limitations should not be overlooked. For instance, there are unavoidable security vulnerabilities in 2G technology, which is still widely used, and which has weak mobile security (Jøsang, Miralabé, & Dallot, 2015). Vulnerabilities in the technology itself and in the capabilities of rapidly developing mobile capabilities must be carefully considered, 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 the adoption of cybersecurity policies to prevent system vulnerabilities, we did not survey the end users, as others have recommended (Karlsson, Kolkowska, & Prenkert, 2016). Since end users are the ones who ultimately make the system work, assessing their attitudes and perceptions of 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 development, implementation, and enforcement of cybersecurity policies for vulnerable systems. We encourage others to study this area, which is beyond the scope of our paper.

Our focus on one particular instance of critical infrastructure may limit the external generalizability of our recommendations. An analysis of vulnerability and resilience in other U.S. critical infrastructures, such as the water system and the electric grid, might lend further insight on how to 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 most portions of critical infrastructure are privately owned, 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 CVD policies were posted; 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 is based on the fear of either criminal or civil repercussions, as has happened with cybersecurity researchers in the past (Doctorow, 2017; Gallagher, 2019; Goodin, 2016). If a CVD policy had been published, and if there was an easily accessible point of contact, we would have followed through and notified the specific municipalities of their potential insecurity. 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 U.S., reporting 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, and 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, possibly incentivizing 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 may be taken to secure the systems they manage. Moreover, as the first academic work to evaluate the current security of EASs and recommend countermeasures that should be considered, we see future research opportunities that could expand to other critical infrastructures at the regional, city, state, and national levels, as well as international critical infrastructure systems, from both academic and practitioner-oriented communities of cybersecurity researchers.

We must secure EASs and be able to inform affected groups when true emergencies occur. The EAS as a whole must be resilient, with authorities recognizing that unintended vulnerabilities will occur, but ensuring 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, starting at the local level and moving to the state, for instance, is one option. A top-down approach, letting the country or the states take the lead and moving down to the local, city, and county municipalities, is also an acceptable approach. We argue that EAS authorities must do something, and they must do it now. Our aging, vulnerable EASs are not equipped to handle potential threats, and we lack sufficient budgeting to find all of the vulnerabilities in the first place. Closing all access to EASs openly available on the Internet is an easy way to strengthen the U.S. EAS, which benefits society as a whole. With a strong EAS cybersecurity plan in place, including proper risk management, CVD policies, encryption of data where possible, testing of systems in the network, sufficient funding, strong private-public-government partnerships, inclusion of end-user training, and prioritizing threats, the U.S. EAS will be made more resilient, thus providing valid, accurate, and timely information to the populations served. The number of cyber criminals attacking EASs is only going to increase; resilient EASs will keep them outside, responding appropriately and according to the cybersecurity plan when the inevitable cybersecurity challenge occurs.

References

Albanesius, C. (2013, July 9). Emergency alert system vulnerable to hackers, report finds. PC Magazine.com. Retrieved from https://www.pcmag.com/article2/0,2817,2421503,00.asp

Attrition. (2016). Legal threats against security researchers: How vendors try to save face by stifling legitimate research. Retrieved from http://attrition.org/errata/legal_threats/

Babinski, A. (2015). State activities in the securing of cyberspace. Internal Security, 7(2), 217-235.

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.

Bonderud, D. (2014, December 26). The responsible disclosure policy: Safeguard or cybercriminal siren song? SecurityIntelligence (Brought to you by IBM). Retrieved from https://securityintelligence.com/the-responsible-disclosure-policy-safeguard-or-cybercriminal-siren-song/

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

Branscombe, M. (2017, January 17). How to handle security vulnerability reports. Cio.com. 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.

Carter, J. G., Carter, D. L., Chermak, S., & McGarrell, E. (2017). Law enforcement fusion centers: Cultivating an information sharing environment while safeguarding privacy. Journal of Police and Criminal Psychology, 32(1), 11-27.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2007). Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. IEEE Transactions on Software Engineering, 33(3), 171-185.

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.

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.

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.

Condit, J. (. (2018, January 4). Arkansas National Guard Conducts Cyber Training Exercise. U.S. Department of Defense. Retrieved from https://www.defense.gov/News/Article/Article/1408321/

Constantin, L. (2013, February 13). Emergency alert system devices vulnerable to hacker attacks, researchers say. ComputerWorld (online). 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, March 14). Military officials testify on cybersecurity on Capitol Hill. U.S. Department of Defense, DoD News, Defense Media Activity. Retrieved from https://www.defense.gov/News/Article/Article/1466442/

Crown, E. (2017, September 8). 'Hacking for Defense' students team with Army to improve casualty care triage. U.S. Army, Medical Materiel Agency. Retrieved from https://www.army.mil/article/193463/hacking_for_defense_students_team_with_army_to_improve_casualty_care_triage

Davis, M. (2015, June 9). Developers: How do you respond to security researcher’s vulnerability reports? . Future Hosting (futurehosting.com). Retrieved from https://www.futurehosting.com/blog/developers-how-do-you-respond-to-security-researchers-vulnerability-reports/

Demer, L. (2018, January 16). Alaska emergency alert system less vulnerable to false alarms than Hawaii’s, officials believe. Anchorage Daily News (online). 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/

Diaz, J. (2012, July 5). This message from NORAD announced global nuclear war—In 1971. Gizmodo.com. Retrieved from https://gizmodo.com/5923528/this-message-from-norad-announced-world-nuclear-war-in-1971

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

Dittmer, J., & Wright, B. (n.d.). Minimizing legal risk when using cybersecurity scanning tools. SANS Institute InfoSec. Retrieved from https://www.sans.org/reading-room/whitepapers/legal/minimizing-legal-risk-cybersecurity-scanning-tools

DoD Vulnerability Disclosure Policy. (2016). Hackerone. Retrieved from https://hackerone.com/deptofdefense

Doctorow, C. (2017, July 24). Security researcher arrested after he warns Hungarian transit company about their dumb mistake. Retrieved March 28, 2019, from https://boingboing.net/2017/07/24/hungarian-messenger-shooting.html

Dodril, T. (2016, May 6). Emergency alert system vulnerabilities could allow terrorists to manipulate a disaster. SurvivalBased.com. Retrieved from http://www.survivalbased.com/survival-blog/7229/emergency-alert-system-vulnerabilities-could-allow-terrorists-to-manipulate-a-disaster/

Dundee Hills Group (2018, October 10). Monroe Electronics to Demonstrate Industry-First Advancements in Emergency Alert Monitoring, Management, and Compliance at SCTE Cable-Tec Expo 2018. Lyndonville, NY. Retrieved fromhttps://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. Retrieved from https://login.proxy.kennesaw.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edslex&AN=edslex80E171CB&site=eds-live&scope=site

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.

Emergency alert system (2018). 83 FR 37750 C.F.R.

Emergency Communications Organization (ECO). (2013). How secure is the US emergency alert system? Satellite. Retrieved from http://www.emergencycomms.org/issue-01/pdfs/articles/emergency-alert-system.pdf

Emergency notification system definitive guide. (n.d.). Keep your people safe, informed, and connected. Alert Media. Retrieved from https://www.alertmedia.com/emergency-notification-system

Fakhoury, H. (2014, April 11). Appeals Court overturns Andrew “weev” Auernheimer conviction – important decision impacts constitutional rights in the Internet Age. Retrieved from https://www.eff.org/press/releases/appeals-court-overturns-andrew-weev-auernheimer-conviction

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

Federal Communications Commission. (2018). Emergency Alert System (No. 2018–15818; pp. 37750–37760). Retrieved from https://www.govinfo.gov/content/pkg/FR-2018-08-02/pdf/2018-15818.pdf

FEMA Fact Sheet. (2007, June 28). Emergency Alert System and Notification (archive). Retrieved from https://web.archive.org/web/20070717212239/http://www.fema.gov/media/fact_sheets/eas.shtm

Fiat, A., & Naor, M. (1993). Broadcast encryption. Paper presented at the 13th Annual International Cryptology Conference, Santa Barbara, California. https://www.iacr.org/cryptodb/data/paper.php?pubkey=1293

Fletcher, M. J. (2016, September 30). The Emergency Alert System test: Lesson learned, catastrophe averted. Network World (online). 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, September 26). The Emergency Alert System: Failure IS an option. Retrieved from https://www.networkworld.com/article/3123778/mobile-wireless/the-emergency-alert-system-failure-is-an-option.html

Frankel, S. E., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W., & Sharma, S. R. (2005). Guide to IPsec VPNs (No. NIST SP 800-77). https://doi.org/10.6028/NIST.SP.800-77

Gallagher, S. (2019, March 26). Casino Screwup Royale: A tale of “ethical hacking” gone awry. Retrieved March 26, 2019, from https://arstechnica.com/information-technology/2019/03/50-shades-of-greyhat-a-study-in-how-not-to-handle-security-disclosures/

Goodin, D. (2016, May 27). Armed FBI agents raid home of researcher who found unsecured patient data. Retrieved March 28, 2019, from https://arstechnica.com/information-technology/2016/05/armed-fbi-agents-raid-home-of-researcher-who-found-unsecured-patent-data/

Hack the Pentagon. (n.d.). Hackerone. Retrieved from https://www.hackerone.com/resources/hack-the-pentagon

Halevy, D., & Shamir, A. (2002). The LSD broadcast encryption scheme. Paper presented at the 22nd Annual International Cryptology Conference, Santa Barbara, California. https://link.springer.com/chapter/10.1007/3-540-45708-9_4

Hausken, K. (2017). Security investment, hacking, and information sharing between firms and between hackers. Games, 8(2), 23.

Hub. (2017, April 12). Hackers put the entire city of Dallas on alert. Hub (online). Retrieved from https://www.hubinternational.com/blog/2017/04/hackers-put-the-entire-city-of-dallas-on-alert/

Hutcherson, K. (2018, March 18). Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand. CNN.com. Retrieved from https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html

ISO/IEC 29147. (2014, February 15). Information technology — Security techniques — Vulnerability disclosure. International Standard. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

ISO/IEC 30111. (2013). Information technology — Security techniques — Vulnerability handling processes International Standard. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-1:v1:en

Jakimoski, K. (2016). Security Techniques for Data Protection in Cloud Computing. International Journal of Grid and Distributed Computing, 9(1), 49–56. https://doi.org/10.14257/ijgdc.2016.9.1.05

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

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, January 13). 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. https://doi.org/10.1109/SURV.2012.121112.00190

Konstantinou, C., Sazos, M., & Maniatakos, M. (2016, 6-8 April 2016). Attacking the smart grid using public information. Paper presented at the 17th Latin-American Test Symposium (LATS), Foz do Iguacu, Brazil.

Kubitschko, S. (2015). The role of hackers in countering surveillance and promoting democracy. Media and Communication, 3(2).

Laszka, A., Zhao, M., Malbari, A., & Grossklags, J. (2018). The rules of engagement for bug bounty programs. Financial Cryptography and Data Security.

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. Paper presented at the 2013 IEEE International Conference on Pervasive Computing and Communications Workshops. https://www.researchgate.net/profile/Tuan_Vuong/publication/261128030_A_taxonomy_of_cyber_attack_and_defence_mechanisms_for_emergency_management_networks/links/56797a2a08aeaa48fa4ab68c/A-taxonomy-of-cyber-attack-and-defence-mechanisms-for-emergency-management-networks.pdf

Lynch, S. (2016, October 15). Full disclosure: Infosec industry still fighting over vulnerability reporting. Cisco Umbrella. Retrieved from https://umbrella.cisco.com/blog/2015/10/16/full-disclosure-infosec-industry-still-fighting/

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. Journal of Strategic Security, 8(5).

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: The Official Publication of the National Guard Association of the United States. Retrieved from http://nationalguardmagazine.com/article/Cyber_Uncertainty/1764536/218066/article.html

Matwyshyn, A. M. (2013). Hacking speech: Informational speech and the First Amendment. Northwestern University Law Review, 107(2), 795-845.

McCool, A. (2017, November 28). Hacking for defense and diplomacy: Steve Blank explains. Raddington Report (online). Retrieved from https://raddingtonreport.com/hacking-for-defense-and-diplomacy-steve-blank-explains/

McFarlane, R. (2017, July 18). Hacking emergency services: How safe is the 911 system?. GCN.com. 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, April 17). 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

Microsoft. (n.d.). Coordinated Vulnerability Disclosure. Microsoft Security TechNet (online). Retrieved from https://technet.microsoft.com/en-us/security/dn467923.aspx

Monroe Electronics. (n.d.). About Monroe Electronics, 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.

Nakashima, E., & Soltani, A. (2014, October 08). The ethics of hacking 101 (posted 2014-10-08 03:20:38). The Washington Post (online).

Nasu, H. (2015). State secrets law and national security. The International and Comparative Law Quarterly, 64(2), 365-404.

Network Installation v. VC3. (2000, November 6). Scott Alan Moulton and Network Installation Computer Services, Inc., Plaintiffs, v. VC3, Defendant. Northern District of Georgia. Retrieved from http://www.internetlibrary.com/pdf/Moulton-VC3.pdf

News, D. (2016, March 31). ‘Hack the Pentagon’ pilot program opens for registration. U.S. Department of Defense. Retrieved from https://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration/

Nixon, R. (2016, April 6). 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

Nunez, K. A. (2017). Negotiating in and around critical infrastructure vulnerabilities: Why the Department of Defense should use its other transaction authority in the new age of cyber attacks. Public Contract Law Journal, 46(3), 663-685.

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

Ochoa, C. (2018, February 26). How grassroots activists in Georgia are leading the opposition against a dangerous “computer crime” bill. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2018/02/how-grassroots-activists-georgia-are-leadin

Ollmann, G. (2013, July 15). Hacking the emergency alerting system. Information Week - DARKReading (online). Retrieved from https://www.darkreading.com/attacks-breaches/hacking-the-emergency-alerting-system/d/d-id/1140113

Osborne, C. (2016, May 9). Security researcher arrested for disclosing US election website vulnerabilities. Zero Day. Zdnet.com. Retrieved from http://www.zdnet.com/article/security-researcher-arrested-for-reporting-us-election-website-vulnerabilities/

Pallotta, F. (2014). Cable customers startled by 'Emergency Alerts.'. CNNMedia (online), 24. Retrieved from http://money.cnn.com/2014/10/24/media/att-alerts/index.html

Paul. (2013, July 12). The Security Ledger. Emergency alert system: Vulnerable systems double, despite zombie hoax. Retrieved from https://securityledger.com/2013/07/emergency-alert-system-vulnerable-systems-double-despite-zombie-hoax/

Peeters, G. (2017, July 7). Strengthening the Achilles heel of the European Union: Make use of ethical hackers to find vulnerabilities in information systems? Leiden University Repository, Masters Thesis. 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).

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

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.

Seals, T. (2017, December 18). Hack the Air Force 2.0 bug bounty kicks off with $10K payout. Infosecurity. Retrieved from https://www.infosecurity-magazine.com/news/hack-the-air-force-20-bug-bounty/.

Seddigh, N., Nandy, B., & Lambadaris, J. (2006). An internet public alerting system: A canadian experience. Paper presented at the 3rd International ISCRAM Conference, Newark, New Jersey. http://www.iscram.org/legacy/ISCRAM2006/ISCRAM2006Proceedingszip/PapersMonday/S2_T1_2_Seddigh_etal.pdf

Serbanescu, A. V., Obermeier, S., & Yu, D.-Y. (2015). A flexible architecture for industrial control system honeypots. Paper presented at the 12th International Joint Conference on e-Business and Telecommunications (ICETE), Colmar, France.

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. Paper presented at the 20th IEEE International Parallel & Distributed Processing Symposium, Rhodes Island, Greece.

Sidner, S., & Andone, D. (2018, January 15). What went wrong with Hawaii's false emergency alert? CNN.com (online). Retrieved from https://www.cnn.com/2018/01/14/us/hawaii-false-alarm-explanation/index.html

Signal. (n.d.). Defense Department launches 'Hack the Army' bug bounty program. Retrieved from https://www.afcea.org/content/Blog-defense-department-launches-hack-army-bug-bounty-program

Storm, D. (2013, July 9). Hackers can hijack unpatched emergency alert system devices, broadcast bogus warnings. ComputerWorld (online). 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.

USAJobs. (2018, March 27-31). Information technology program manager (Policy and planning/information security). Department of the Army. Retrieved from https://www.usajobs.gov/GetJob/ViewDetails/495022600

U.S. Census Bureau (2019). https://www.census.gov/

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.

Whitaker, Z. (2018, March 27). Atlanta, hit by ransomware attack, also fell victim to leaked NSA exploits. CNN.com. Retrieved from http://www.zdnet.com/article/atlanta-hit-by-ransomware-attack-also-fell-victim-to-leaked-nsa-exploits/

Wimberly, R. (2014, December 9). Emergency alert system's complex vulnerability issues. Emergency Management (online). Retrieved from http://www.govtech.com/em/emergency-blogs/alerts/Emergency-Alert-Systems-Complex-Vulnerability-Issues.html

Wireless RERC. (2016). Observations of the 2016 National EAS Test. Research Brief. Rehabilitation Engineering Research Center for Wireless Technologies (Wireless RERC), sponsored by the National Institute on Disability, Independent Living, and Rehabilitation. 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 Instrumentaion & 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 (bepm). PLoS One, 10(12), 1-11.

Yasin, R. (2016). So you want to be a security researcher?. Information Week – DarkReading. Retrieved from https://www.darkreading.com/careers-and-people/so-you-want-to-be-a-security-researcher/d/d-id/1324453

Yerak, B. (2015, January 04). FBI seeking 'ethical' hackers. c. Telegraph – Herald, 89.

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 Index Quarterly, 18(4), 279-291.

Zetter, K. (2016). Appeals Court overturns conviction of AT&T hacker 'Weev'. Wired.com. Retrieved from https://www.wired.com/2014/04/att-hacker-conviction-vacated

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 Ph.D. 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. Green 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 Ph.D. 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. Ms. Dodson earned her Bachelor of Business Administration degree in Information Security and Assurance. In 2018, Ms. Dodson was selected as the “ISA Student of the Year” by department faculty, in recognition of her outstanding academic performance. After graduation, Ms. Dodson 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. Mr. Easton earned his Bachelor of Business Administration degree in Information Security and Assurance. After graduation, Mr. Easton took a position as an infrastructure engineer with a large defense contractor, based in the Washington D.C. area.