Improving Protection Against Cybersecurity Attacks of Emergency Dispatch Centers

James Sweeney and Vu Tran
Capella University, MN, USA
Jsweeney1@capellauniversity.edu
vu.tran@capella.edu

Abstract: Public service answering points (PSAPs), also known as 911 dispatch centers, serve as integral and critical infrastructure components that serves as a conduit between the public and emergency assistance such as police, fire and emergency medical services. It has been demonstrated in previous research, that PSAPs may be exceptionally vulnerable to telephonic and distributed denial of service (TDoS/DDoS) attacks with potentially devastating effects. It is the purpose of this study is to gather the best practices from experts and tap into the knowledge of the professionals tasked with safeguarding PSAPs every day. Due to the unknown full capabilities of the PSAPs and the antiquated infrastructure on which they must operate, it is unclear just what safeguards are in place to defend these critical infrastructure components against attacks of this nature. To gather this information, a multiple rounds qualitative Delphi study was conducted. Through this process, participants were asked to comment on current tactics and techniques, practices that could be implemented under ideal conditions without political or financial hurdles and how to bridge the gap between current and optimal environments. PSAP administrators, hereby referred to as experts, with a minimum of five years of experience working within a United States PSAP were included in this study and provided a firm understanding of their capabilities. The suggestions provided by participants included patch managements, updated hardware, federally mandated standards, regular plan exercises, and standardized education. After gathering and analysing the data, three basic tenets could be appreciated including cyber hygiene, preparedness and intelligence, and education and training. It is expected that the results of this study will prove integral in not only better securing the PSAPs within the United States critical infrastructure, but also understanding some of the hurdles and difficulties PSAP administrators must overcome.

Keywords: 911 Dispatcher Center, DDoS, TDoS, 911 communications center, PSAP, Public Service Answering Point

1. Introduction

Public service answering points (PSAPs), also known as 911 dispatch centers, serve as the gateway for those needing to access emergency assistance from police, fire, and emergency medical services (FCC, 2021). The delivery of emergency services through the 911 system is crucial for ensuring health, safety, and welfare of the public. The proper emergency services are dispatched after the caller communicates with a telecommunications officer at their local PSAP. In the United States, users can dial 911 and be immediately put in contact with telecommunicators (i.e., dispatchers) who provide pre-arrival instructions and allow early treatment and intervention be administered before the arrival of emergency units (FCC, 2021). According to the National Emergency Number Association (NENA), an estimated 240 million 911 calls are placed in the United States every year, with approximately 80% being placed via wireless devices (NENA, 2021). Calls for assistance are directed through primary and secondary PSAPs equipped with personnel trained to provide emergency assistance and serve as a conduit between the caller and the field unit (FCC, 2021).

As technology advances, PSAPs are beginning to transition to the Next Generation 911 (NG911) systems, which are Internet Protocol (IP) based. This allows for the transmission of text messages and Voice-over-IP (VoIP) calls to be seamless through the 911 network (911.gov, 2016). This allows a caller to summon help when they might not otherwise have been able, for instance when being followed and cannot call without putting themselves at risk. Even though this added functionality lowers the threshold for access, it introduces a significant vulnerability for cyber-attack (Kang, Gilgor, & Sekar, 2017). The upgrading of this system is estimated to cost over $10 billion and anticipated to take multiple years (Jackson, 2017). The cybersecurity challenges to PSAPs are here today, yet the realization of the NG911 is years away. Due to the critical nature of the 911 service, a cybersecurity solution to bridge the gap between today's system and NG911 is needed (APCO International, 2017).

The purpose of this qualitative Delphi study is to gather the best information security practices of experienced professionals safeguarding PSAPs daily. From that data, a model can be developed to be used by PSAPs nationwide until NG911 become available. Today's PSAPs are based on an antiquated architecture that has been in place since the 1970s (Jackson, 2017). The lessons learned from this intermediate step will provide valuable information and help foreshadow potential issues to avoid during the implementation of the new infrastructure. This model can be used as a vehicle to finetune the viability of the long-term solution. Our research question:

What model can be developed to better safeguard PSAPs against cyber-attacks while they still function using the current antiquated architecture?

2. Background

According to the NENA, an average of 650,000 emergency calls for assistance are placed through PSAPs daily (NENA, 2021). Calls are placed via landline or cellular device through their respective infrastructures (Guri, Mirsky, & Elovici, 2016). The 911 network serves as an entry point and conduit for the public to access the emergency services system. It has become a vital component to emergency response and disaster preparedness, functioning as a backbone that enables field units to receive and convey crucial information (FCC, 2021). Public service answering points have been recognized as a component of the critical infrastructure sectors through the Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act; USA Patriot Act, 2001). Furthermore, the communications sector is unique, as its failure has the potential to affect multiple other sectors (White House, 2013).

The current infrastructure on which PSAPs rely was initially developed in the 1970s and is antiquated compared to current day standards and must be updated to get on par with what everyday citizens can do with a smartphone (Jackson, 2017). Researchers from Ben-Gurion University of the Negev Cybersecurity Research Center (Guri et al., 2016) conducted a study to determine how vulnerable a PSAP is to a telephonic denial of service (TDoS) attack, and the devastating effects should an attack be successful. A botnet consisting of approximately 6,000 bots could launch a TDoS attack paralyzing the PSAPs in a state the size of North Carolina for days (Guri et al., 2016). Furthermore, a botnet consisting of approximately 200,000 bots using the same attack would have the ability to affect the 911 system throughout the entire country. As the abilities and functionalities of botnet variants continue to grow, this possibility becomes increasingly real. As of 2017, over 40% of PSAPs and critical infrastructure sectors have experienced some level of cyberattack (Seals, 2017). The federal government is taking steps to develop tools that may be implemented to defend these assets against such attacks. It is reported that one out of 300 emails to public administration contain malicious data with 184 cyber-attacks made on the public sector from 2016-2018 (Motorola, 2019).

The money needed to upgrade the system is substantial and therefore prohibitive. The Association of Public-Safety Communication Officers (APCO) reports a substantial grant program from Congress and many years are needed to accomplish this initial upgrade (Jackson, 2017; Kang et al. 2017). It is estimated at least $10 billion is needed to provide all PSAPs nationwide with the resources needed to enhance their systems and ensure proper mechanisms are implemented (Jackson, 2017). This situation requires that a solution be developed and implemented to bridge today's infrastructure to the proposed NG911 infrastructure. To facilitate this, the Cybersecurity and Infrastructure Security Agency (CISA), in conjunction with the SAFECOM-NCSWIC Next Generation 911 working Group, relies on stakeholder feedback to develop and innovate new concepts to safeguard the 911 Communications System (CISA.gov, 2021). CISA has also developed several resources highlighting the vulnerability of the 911 system and how to enhance the overall cybersecurity (CISA-Transition, 2021).

A challenge we face in search for a bridge gap solution for PSAPs problem is the lack of uniformity in practices and techniques currently used in PSAPs. As the result, we decided to focus this study on understanding best practices at these PSAPs.

3. Methodology

A qualitative Delphi method was utilized for our study. This method relies on an iterative interview process to develop a consensus among the participants of the study (Skulmoski, Hartman, & Krahn, 2007). Multiple rounds of interviews were conducted, with feedback interspersed between each round. The process completed when consensus was reached among participants (Skulmoski, Hartman, & Krahn, 2007). If there were disagreements that could not be resolved, the disagreements were recorded. With each new round, new questions were developed based on the responses from the previous round and presented to participants to build consensus. Our role as researchers is to facilitate the consensus building process. During the interview process, we focus on clarifying the interview process, asking the interview questions, collecting responses, and disseminating results for participants' approvals. We point out the disagreements among participants to help facilitate a resolution. All communications are strictly between individual participants and the facilitators. Participants do

not directly engage each other during the interview. Convergence was reached when there was a final agreement on a list of security measures for PSAPs or when no further consensus can be reached.

According to Hasson, Keeney, & McKenna (2000), study's validity using a qualitative Delphi method is assured by several mechanisms. The method relies on a collaborative decision-making process involving multiple participants which is more likely to yield correct outcomes than a single person. Decisions are subject to multiple rounds of reviews and challenges to further enhance their validity. The use of subject-matter experts as participants strengthens decision validity. Keeping participants from directly engaging each other during the rounds of interview helps prevent the risk of early decision convergence due to peer pressure.

The Delphi methodology has been used to develop models within the cybersecurity space before. Karabacak, Yildirim, and Baykal (2016) developed a model that could be used to measure the readiness of national critical-infrastructure protection efforts based on a grounded theory evaluation of national cybersecurity projects. Turoff, Bañuls, Plotnick, Hilitz, and Ramírez de la Huerga (2016) used the same methodology to develop a single model exhibiting the collective viewpoints regarding the interactions of emergency managers and critical infrastructure conditions. Seppãnen, Luokkala, Zhang, Torkki, and Virrantaus (2018) queried participants through a Delphi study that examined the interdependencies between the failures of critical infrastructures as perceived by regional preparedness committees. Kong, Kim, and Lee (2017) conducted a Delphi study to create a model that can be used to classify cyber-attackers and evaluate their capabilities.

3.1 Participants

Below are the participation criteria:

- PSAP administrators, supervisors, and decision-makers responsible for deciding cybersecurity techniques and tactics best used securing their centers. These participants' daily function is to oversee the security and operation of the PSAP systems and have an intricate understanding of how each supporting system interacts.
- Administrators who have worked in their respective positions for at least five years.
- Administrators who have worked at PSAPs within the United States.
- Participants must currently hold a basic telecommunicator certification (BTC) or equivalent, with preference given to those possessing emergency medical dispatch certifications.
- Participants must be willing and able to voluntarily participate from the study's beginning until the end. Participants who withdraw from the study early will have their interview data removed from the study.

We looked for 15 PSAP professionals to participate. This number met the recommendation of between 10 to 50 participants (Iqbal & Pipon-Young, 2009). The following steps were taken during the recruitment process:

- A presentation reviewing the study was provided to state-wide Emergency Medical Services 911 sub-committee meeting. The terms and conditions of permissions and ethical considerations were provided.
- PSAP administrators were found and contacted through LinkedIn. The same information from the initial presentation was conveyed to these potential participants.
- Potential participants who express interest were vetted by the researcher to ensure compliance with the requirements.
- All participants were contacted and notified whether they qualify. If qualified, additional information was provided regarding when the study was scheduled to be performed.

Before conducting the study or asking any questions, consent forms were obtained electronically.

3.2 Setting

A search on LinkedIn was completed to access participants nationwide. Names, locations, and agency affiliation of the participants were withheld for security purposes. The setting for the first three rounds of the interview was done using a combination of online survey, specifically SurveyMonkey® and emails. The fourth round was conducted via Zoom and phone interviews.

3.3 Analysis of Research Questions

Three main interview questions were posed to participants in Round One interviews:

- What cybersecurity standards and techniques (both internally and externally) have you implemented to secure your PSAP against cyber-attacks?

- In an ideal world in which finances, politics, and dated infrastructure were not issues, what other techniques and tactics would you like to see implemented to better safeguard your PSAP against cyber-attacks while still operating using the current network infrastructure?
- With the gap identified and working with the current infrastructure, what steps can be taken that would better protect PSAPs from potential cyber-attacks, and what would it take for you to implement these practices?

4. Data Collection and Analysis

The responses to Round One of the interviews were open-ended to allow participants freedom to explain and expand upon their responses. The open-ended responses received from SurveyMonkey were entered into NVivo 12 (NVivo, n.d.) for data coding and content analysis. Participant responses were reviewed and categorized according to the topic of the response. For example, one response recommended firewalls, strong passwords, and anti-virus protections. This response was coded once for firewalls, once for passwords management and another for anti-virus protection. Emerging patterns and themes were developed to guide the development of interview questions in subsequent rounds. Responses to these subsequent interview questions allowed the researcher to further refine the patterns and themes from the previous round into concrete security measures. Through the process of consensus building over several interview rounds, researchers developed the final list of security measures for enhancing existing PSAPs. Within each round of interviews, the participants were provided with the following:

- A report and explanation of the response analysis from the previous round.
- Items as uncovered in the previous round to be further evaluated in the next round.
- For each item identified, an aggregated score representing the collective agreement of participants agreeing with the item from the previous round.
- A list of questions for exploration and expectations of the new round of interview.

The participants provide responses to the interview questions in each round. For Round One, Two, and Three, written responses were provided. For Round Four, Zoom or phone calls were used.

5. Findings

5.1 Participants

Seventeen potential participants responded, with one participant not meeting the length of service requirements. Instead, that person passed the survey to someone else (P9) who did fit the requirements. P17 responded with interest but decided to not participate due to time constraints. Data collection began with 16 participants, which allowed for the loss of some participants should some decide not to participate. The rounds were continued until a minimum of 10 participants responded.

Table 1 Description of Potential Participants

Identifier	Role	Years	Within US	Certification
P1	PSAP Administrator	20+	YES	YES
P2	PSAP Administrator	5+	YES	YES
P3	Communication Supervisor	5+	YES	YES
P4	CAD Administrator	10+	YES	YES
P5	Communications Division Manager	10+	YES	YES
P6	Assistant Director	10+	YES	YES
P7	PSAP Administrator	30+	YES	YES
P8	System Analyst	5+	YES	YES
P9	Director	15+	YES	YES
P10	Executive Director	NO	YES	YES
P11	Emergency Communications Center Manager	10+	YES	YES
P12	911 Communications Technical Systems Coordinator	10+	YES	YES
P13	State 911 Program Manager	15+	YES	YES
P14	PSAP Administrator	10+	YES	YES
P15	PSAP Administrator	25+	YES	YES
P16	Director of Information Technology	10+	YES	YES
P17	Emergency Communications Specialist	5+	YES	YES

5.2 Round One Interview Results

Each participant provided the researchers a list of responses for each interview questions posted on SurveyMonkey®. The researchers collected and distributed all the responses to all participants via email. Participants were asked to review all the responses and categorize them into core themes. Researchers reviewed the themes and suggested how they can be organized. Except for their own responses, the participants do not know the owners of other responses. The responses to all three questions were categorized into the several core themes by the participants after several rounds of email exchanges (Table 2).

The final set of themes were presented via SurveyMonkey as a survey for participants to vote. Participants were asked to elaborate on each theme as to what security measures they previously implemented along the themes identified. Table 3 captures the participants' responses regarding specific security measures implemented in the context of the common themes identified from their responses to our Question 1. A total of 64 suggestions were gathered through participant interviews. Participants were also asked to categorize these security measures (Table 3, Column 2).

Table 2: Themes Generated by the Participants to Questions 1, 2, and 3 of Round One Interview

Item	Based on Question 1 Responses	Based on Question 2 Responses	Based on Question 3 Responses
1	Properly configured Firewalls	Implementation of defense in depth methodology such as use of redundant firewalls, independent intrusion detection monitoring systems.	A statewide security operations center to monitor all PSAP systems.
2	Maintaining multiple ISPs	Complete separation of network infrastructure at all levels.	Accepted best standard.
3	External devices prohibited in the towers	Dedicated IT person.	Federal mandate.
4	Network isolation	Nothing can be done on this current platform.	No idea / there is nothing that can be done.
5	Limited Internet access	ESINet Migration.	Education and training (including tabletop drills).
6	Control traffic flow	State-wide cybersecurity program to coordinate efforts and provide training.	Secure network (network isolation, disabling unused ports, etc.)
7	Limit Admin access	Additional network monitoring outside of firewall.	Strong vulnerability assessments.
8	Traffic monitoring via port and IP address	Better virus scanning.	Information sharing among PSAPs.
9	Redundancy	Public safety only DNS servers geographically separated.	Frequent good vulnerability assessments.
10	Use of a VPN to secure data	Stiffer laws and penalties.	Active monitoring.
11	Incident response plan development	Updated server OS.	Funding.
12	Strong password standards	Network monitoring.	External expertise to supplement internal resources and personnel.
13	Anti-virus protection	Implementation of defense in depth methodology such as use of redundant firewalls, independent intrusion detection monitoring systems.	System redundancy.
14	Internet of Things Awareness training	Complete separation of network infrastructure at all levels.	The best fire walls possible to protect the 911 network as we move into NG
15	Implementation of NIST Framework	Dedicated IT person.	Enhanced and upgraded equipment (Specifically firewalls).

Table 3: Themes identified from Question 1 (with Votes) by Participants

Response	Vote
Properly configured firewalls	3
Maintaining multiple ISPs	3
External devices prohibited	3
Network Isolation	3
Limited Internet access	2
Control traffic flow	2
Limit admin access	2
Traffic monitoring via port and IP address	2
Redundancy	1
Use of a VPN to secure data	1
Incident response plan development	1
Strong password standards	1
Anti-virus protection	1
Internet of Things Awareness training	1
Implementation of NIST Framework	1

Table 4: Security Measures in Responses to Question 1, with Category

Security Measure	Category
Administrative Internet access	Admin Access
Access to the systems is controlled via security log on	Admin Access
Anti-virus protections	Anti-Virus
No other items are permitted to be plugged into towers	External Devices
Do not allow flash drives or other input devices	External Devices
USB port restrictions	External Devices
Firewalls	Firewall
Firewalls on critical servers	Firewall
Firewall monitoring	Firewall
Incident response plans	Incident Planning
Internet access is disabled	Limited Internet
No external Internet access	Limited Internet
Internet of Things Awareness	Education
Systems are on their own networks	Isolation
Computers are closed off from Internet	Isolation
Network is isolated with implicit deny rules in the firewall	Isolation
Just started implementing some NIST	NIST
Rollover of incoming 911 calls	Redundancy
Security against TDoS attacks are handled through our 911 System service provider	Service Provider
Maintaining multiple ISP connections	Service Provider
Separate paths and different ISPs	Service Provider
Strong password standards	Strong Passwords
One-way connection	Traffic Flow
Only servers have outgoing access	Traffic Flow
Appliances at the edge that monitor traffic	Monitor
Active monitoring outside the firewall.	Monitor
Our IT department has installed VPN	VPN

This process for arriving at common themes was the same for Questions 2 and 3. The resulting security measures are summarized in Tables 4 and 5.

Table 5: Security Measures in Responses to Question 2, with Category

Security Measure	**Category**
Complete separation of network infrastructures	Network Isolation
Further segmentation of the administrative network	Network Isolation
Having an IT person who is a department employee	Personnel
A staffed NOC allowing technician to be notified	Personnel
Inhibit the external access to internal systems	Defense in Depth
Multiple redundant firewalls… fully automatic patch monitoring	Defense in Depth
Additional sensors on the network with more advanced IDS	Defense in Depth
Public safety only DNS server	DNS
This person would provide needed training	Education

Security Measure	Category
Preparing to migrate to an ESInet	ESINet
I would like network monitoring	Network Monitoring
Not sure there is a good solution for TDoS	Nothing
Implement a state-wide cybersecurity program	State-wide program
Better laws, stiffer penalties	Laws
Updated server operating systems	Updates
Better virus scanning	Defense in Depth

Table 6: Security Measures in Reponses to Question 3, with Category

Security Measure	Category
It takes active monitoring	Monitoring
Education and training is vital	Education
Provide cyber security training	Education
Best firewalls possible to protect the 911 network	Firewall
State level funding	Funding
It is going to take funding	Funding
Federal mandate and funding	Funding
Funding and external expertise	Funding
Sharing real time information	Info Sharing
Standard that is backed by a federal mandate	Mandate
External expertise to supplement internal resources	Personnel
It takes active monitoring and knowledgeable people	Personnel
It is going to take funding and redundancy	Redundancy
It would take an accepted best standard	Standard
Statewide security operation center	Statewide center
Good vulnerability assessments	Assessments
Secure network, disabling unused workstation ports	Cyber Hygiene
Continual monitoring and upgrades/updates	Updates

5.3 Round Two Interview Results

During Round Two interview, participants were asked to confirm whether the suggestions gathered in Round One were acceptable. Of the 10 Round Two responses, 90% of the participants agreed the suggestions were acceptable. One participant stated they were not but did not offer any reasoning why or offer any additional suggestions. Once the list was accepted, some themes became increasingly obvious.

During the analysis, three overarching categories could be noticed. A vast majority of the suggestions were based on employing strong cyber hygiene practices like network monitoring, system redundancy, virus scanning, and password standards. A total of 41 of the 64 suggestions could be categorized as cyber hygiene practices, representing a percentage of 64.0625% of suggestions, shown in Table 6. Other suggestions spoke to the preparedness and intelligence of the PSAP and its ability to respond to an incident. This category included suggestions such as frequent and strong vulnerability assessments, state-wide coordination efforts, and information sharing among PSAPs. A total of 17 suggestions could be categorized under preparedness and intelligence, resulting in 26.56%, shown in Table 7. Finally, education/training was another theme that was appreciated through participant suggestions. Three suggestions spoke to standardized awareness training, representing 4.6875% of the total number of suggestions, shown in Table 8.

Table 7: Cyber Hygiene Category

Category	Number
Complete separation of network infrastructure at all levels.	7
Additional network monitoring outside of the firewall.	4
Properly configured firewalls	4
Limited Internet access	4
Multiple Internet Service Providers to increase bandwidth.	3
External devices prohibited in towers	3
Enhanced and upgraded equipment	3
Improved virus scanning.	2
System redundancy	2
Control of traffic flow	2
Implementation of defense in depth methodology	2
VPN Use to secure data	1

Category	Number
Strong password standards	1
Implementation of NIST framework	1
Geographically separated, public safety specific, DNS servers	1
Updated server operating systems	1
TOTAL	41
PERCENTAGE	64.0625%

Table 8: Preparedness & Intelligence

Category	Number
Funding	4
External participants to supplement internal resources and personnel	4
State-wide cybersecurity program to monitor and coordinate efforts	2
Frequent and strong vulnerability assessments.	2
Information sharing among PSAPs.	1
Stiffer laws and penalties for bad actors.	1
Federally mandated cybersecurity protocols.	1
Accepted best practice and standards.	1
Incident response plan development.	1
TOTAL	17
PERCENTAGE	26.56%

Table 9: Education & Training

Category	Number
Incident plan education, training and exercising	2
Standardized training	1
TOTAL	3
PERCENTAGE	4.6875%

5.4 Round Three and Round Four Interview Results

In Round Three and Four, participants were asked whether they agreed with these categories and if they would make any additional suggestions or changes. Out of all the responses, all participants agreed with the recommendation organization or content. Some participants failed to provide an answer to some of the questions. 10 participants remained through the entire interview process. The consensus reached among these participants was around 80% across all three interview questions provided.

Table 10: Agreements to the Round Two Results

Response	Question 1	Question 2	Question 3
Yes	8	8	7
No Answer	2	2	2
% In Agreement	80.00%	80.00%	77.78%

5.5 The Model

According to Turoff, et al., a model is a tool that outlines a process for implementing a strategy to solve a problem (Turoff, Bañuls, Plotnick, Hilitz, & Ramírez de la Huerga, 2016). Based on the data gathered, the model proposed contains three areas of cybersecurity improvements including, Cyber hygiene, preparedness & intelligence, and education & training. It is surmised implementation of this model can assist PSAP administrators in securing centers against cybersecurity threats in the near term as they wait for the NG911 technology be implemented and infrastructure upgraded. The safety measures for each area of the model is listed in Tables 7, 8, and 9.

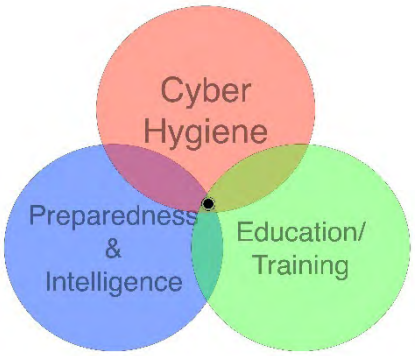

Figure 1: Cybersecurity Model for PSAPs

6. Discussion, Recommendations and Conclusions

6.1 Discussion

The purpose of this study was to tap into the expert knowledge of participants to gain a consensus on techniques and tactics that could be used to develop a model for addressing near term security needs of PSAPs. Our model identifies three safety measure areas: cyber hygiene, preparedness and intelligence, and education and training. Cyber hygiene includes common cybersecurity practices like defense in depth, strong password requirements, and network isolation. Preparedness and intelligence encourage PSAP administrators to share information and work collaboratively in defending against cyber-attacks. Finally, education and training provide a standard for all telecommunicators and management to better protect this infrastructure.

6.2 Recommendations

The model developed provides insights into the near-term security measures needed by today's PSAPs. This model can be used as a check list for analyzing the cybersecurity readiness of each operating PSAP center in the United States. The model can be used to help prioritize the implementation of security measures in the NG911 program rolled out in the future. The model can be used in reviewing historical data on PSAP attacks to identify potential gaps between what attacks performed and what security protections the model recommends.

This study should only be considered the starting point as further studies are needed to validate the model. Our study relies on the opinions and consensus of a panel of ten PSAP professionals. Additional interviews with PSAP professionals can help further confirm the model's list of security measures. Reviewing the list of security measures captured in the model against security standards such as NIST will allow identification of gaps between the model and the general recommended best practices, allowing opportunities for improving the model. Conducting a similar study with service providers may provide insight on the ability to defend PSAPs against TDoS/DDoS attacks specifically.

6.3 Conclusion

PSAPs are an integral component of the emergency services system in the United States. Disruption of the PSAPs can result in loss of lives. Cyberattacks of PSAPs is a real problem today, as over 40% of PSAPs and critical infrastructure sectors have already experienced them (Seals, 2017). Recognizing the near-term risk, the Department of Homeland Security, Science, and Technology Directorate (S&T) funded two research programs to harden defenses against DDoS and TDoS attacks. Whether PSAPs upgrade their current systems to include the NG911 concept or a major infrastructure upgrade is made, security measures are needed across all PSAPs. Implementation of this model is applicable regardless of the status of the PSAP infrastructure. Our security model captures the recommended cybersecurity best practices for protecting the PSAPs in the near term.

References

911.gov. (2016). *Next Generation 911*. U.S. National Highway Traffic and Safety Administration. Retrieved on November 28, 2017 from https://www.911.gov/issue_nextgeneration911.html

APCO International. (2017). *Broadband implications for the PSAP: Analysing the future of emergency communications*. APCO International. https://www.apcointl.org/download/apco-p43-report/?wpdmdl=5984&ind=0

CISA. (2021). Next Generation 911 Publications. Retrieved on November 27, 2021 from https://www.cisa.gov/publication/next-generation-911

CISA-Transition. (2021). Transition to Next Generation 911. Retrieved on November 26, 2021 from https://www.cisa.gov/safecom/next-generation-911

FCC. (2017). *911 and E911 services.* Federal Communications Commission https://www.fcc.gov/general/9-1-1-and-e9-1-1-services

Felicity Hansson, Sinead Keeney, and Hugh McKenna (2000). Research Guidelines for Delphi Survey Technique. Journal of Advanced Nursing, 32(4), 1008-1015.

Guri, M., Mirsky, Y., & Elovici, Y. (2016*). 911 DDoS: Threat, analysis and mitigation.* Ben-Gurion University of the Negev Cyber-Security Research Center. https://arxiv.org/ftp/arxiv/papers/1609/1609.02353.pdf

Iqbal, S., & Pipon-Young, L. (2009). *The Delphi method.* Retrieved July 28, 2018 from https://thepsychologist.bps.org.uk/volume-22/edition-7/delphi-method

Jackson, D. (2017). APCO identifies potential NJ911 impacts, challenges in Project 43 report. *Urgent Communications*. Littleton.

Kang, M., Gilgor, V., & Sekar, V. (2017). Defending against evolving DDoS attacks: A case study using link flooding incidents. *Springer International Publishing, (24),* 47-57.

Kong, M., Kim, N., & Lee, G. (2017). AHP and Delphi method-based attack-capability evaluation methodology. *International Information Institute (Tokyo). Information, 20*(9A), 6497-6509.

Motorola. (2019). Secure Next Generation Systems and Secure the PSAP. Retrieved on November 26, 2021 from https://www.vestapublicsafety.com/pdf/Secure-the-PSAP-Whitepaper.pdf

NENA. (2017). *NENA master glossary.* Retrieved March 7, 2018 from https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-ADM-000.22-2018_FINAL_2.pdf

NENA. (2017). *911 statistics.* Retrieved November 26, 2021 from https://www.nena.org/?page=911Statistics

NENA. (2017). *NENA master glossary of 911 terminology; NENA-ADM-000.21-2017*. Retrieved November 28, 2017 from https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/standards/NENA-ADM-000.21-2017_FINAL_2.pdf?hhSearchTerms=%22definition%22

NVivo. (n.d.). *NVivo.* Retrieved January 5, 2019 from https://www.qsrinternational.com/NVivo/home

SAFECOM. (2019). Cyber Risks to Next Generation 911. Retrieved on November 27, 2021 from https://www.cisa.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer.pdf

Seals, T. (2017, March 29). *40% of ICS, Critical infrastructure targeted by cyberattacks*. Retrieved October 19, 2017 from https://www.infosecurity-magazine.com/news/40-of-ics-critical-infrastructure/

Seppãnen, H., Luokkala, P., Zhang, Z., Torkki, P., & Virrantaus, K. (2018). Critical infrastructure vulnerability – A method for identifying the infrastructure service failure interdependencies. *International Journal of Critical Infrastructure Protection, 22,* 25-38. doi:10.1016/j.ijcip.2018.05.002.

Skulmoski, J., Hartman, G. T., & Krahn, J. (2007). The Delphi method for graduate research, *Journal of Information Technology Education: Research, 6,* 1-21. doi:10.28945/199.

Turoff, M., Bañuls, V. A., Plotnick, L., Hilitz, S. R., & Ramírez de la Huerga, Miguel. (2016). A collaborative dynamic scenario model for the interaction of critical infrastructures. *Futures, 84,* 23-42. doi:10.106/j.futures.2016.09.003.

USA Patriot Act. (2001). Pub. Law 107-56, 107th Congress.

White House. (2013, February 12). *Presidential Policy Directive – Critical infrastructure security and resilience.* Retrieved January 24, 2018 from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil