

Mitigating Swatting Events in the Healthcare Sector



IAHSS
FOUNDATION

*Dedicated to Research and Education
in Healthcare Security and Safety*

IAHSS-F RS-23-01

April 1, 2023

***Evidence-Based
Healthcare Security
Research Series***

IAHSS Foundation

The International Association for Healthcare Security and Safety (IAHSS) Foundation was established to foster and promote the welfare of the public through education and research and the development of a healthcare security and safety body of knowledge. The IAHSS Foundation promotes and develops research to further the maintenance and improvement of healthcare security and safety management, and it develops and conducts educational programs for the public. For more information, please visit www.iahssf.org.

The IAHSS Foundation is completely dependent on the charitable donations of individuals, corporations and organizations. Please help us continue our mission and our support of the healthcare industry and the security and safety professionals who serve institutions, staff and, most importantly, patients. To donate or to learn more about the IAHSS Foundation, please visit the website or contact Nancy Felesena at (888) 353-0990.

Thank you for your continued support.

Ronald Hawkins
Research Committee Chair
IAHSS Foundation

IAHSS Foundation Board of Directors

Bonnie Michelman, President
Massachusetts General Hospital

Marilyn Hollier
Security Risk Management Consultants

Dan Yaross, Treasurer
Security Risk Management Consultants

Bill Navejar
Consultant

Paul Greenwood
Unity Health Toronto

Steve Nibbelink
Secure Care Products

Ronald Hawkins
Security Industry Association

Brigid Roberson
Texas Medical Center

Scott Hill
King's Daughters Health System

INTRODUCTION

Swatting involves a person making a false report to emergency services or 911 in order to elicit a response to dispatch a team of police or specialized units such as a SWAT team. Swatting can impose a problem of diverting necessary resources to actual emergencies or to intimidate health professionals. Additionally, disruption of hospital operations causes distress for everyone involved. It is important for hospitals to recognize the possibilities of a swatting call and develop safety protocols to address this risk and maintain the safety and security of all involved.

Swatting, in many cases, is deemed as a form of online harassment in the United States. There are many definitions of swatting, but in the context of healthcare, swatting may come in incidences where an individual reports falsely of either a medical emergency (e.g., overdose, heart attack), or other dangerous circumstances that would result in sending out law enforcement. In a general definition that is widely used, the act of swatting consists of an individual calling the police, identifying as somebody else who is perpetrating a situation that is almost certainly going to lead to the loss of innocent lives, such as an armed hostage situation (Lamb 76). Though both definitions can occur in or out of the hospital setting, both yield similar results as there is a probable likelihood of the endangerment of the parties involved. Swatting can sometimes be done solely for the purpose of revenge or to play as a prank, but nevertheless, is considered a heinous crime and can have the potential to result in deadly consequences.

METHODS OF SWATTING

There are many channels that can be used to obtain information in order to execute swatting. Swatting calls are done by individuals who are already widely familiar with technology. One common form that is widely used is social media. Social media comes in many platforms such as Facebook, Instagram, Snapchat, Twitter, or others that enables a user to be easily accessible to a plethora of information just by identifying someone's name. By gathering such information, it makes it more likely that they are able to contact through texting, calling, or emailing a swatting threat. VPN, otherwise known as a virtual private network, is utilized to create an encrypted connection over a network that is less secure, which is typically our internet. This network is used as opposed to a wide area network (WAN) because it is more cost-friendly (Pavlicek & Sudzina 2018). VPN's protect against cybercrime on insecure networks while also providing privacy for users. Virtual private networks essentially give protection for all users on the internet by enforcing authentication through means of passwords and identification.

In cases of swatting, Caller ID spoofing is a related issue. Spoofing technology enables the user to cover their own personal numbers and substitute it with the victim's number, which makes it possible for dispatchers to be fooled. Caller ID is a service given from telephone operators where the phone number and/or name of the caller is transmitted to the recipient (Mustafa et al, 1). This is done in order to give an informed consent to the

recipient to answer these calls being transmitted from both channels. Though this service presents measures for users to become aware of the caller, there are still notable concerns regarding the security and accessibility. In settings such as a hospital, it is natural for calls from patients to be answered, so it is difficult to determine whether these calls are a hoax or are genuine. The internet makes it easier to access contact information for hospitals. As a result, there is no distinction between whether calls are made as a prank or emergency. There are existing applications that can also be downloaded on one's device easily to spoof caller information or by using service providers as well. Even if there are attempts to end these spoof calling attacks, the necessary upgrades to the hardware are very costly (Mustafa et al, 1). Through usage of applications or dialing numbers, there is no accurate authentication of these users.

No current protocols are in place to help hospitals identify caller ID spoofing. Hospital dispatchers are more likely deceived because they treat every call as an emergency. Absence of procedures underscores the likelihood of a swatting attack occurring. If there were strategies implemented to strengthen verification processes, and recognizing traits of spoofing attacks, then callers will be less encouraged to communicate threats and potential harm to the patients and health professionals.

SWATTING INCIDENTS

Many of the instances of swatting that have been committed have resulted in many lost lives and resources. Nathan Hanshaw was sentenced to thirty months after placing swatting calls towards multiple states which had ended up in numerous road closures and evacuations in buildings. An event like this not only wasted the efforts of law enforcement, but also caused panic to all that was affected by these swatting threats. Similarly, an individual named Mir Islam was also sentenced to twenty four months in prison for committing swatting and doxxing multiple victims. Zachary Lee Morgenstern made several swatting calls and texts which had ended in his punishment of forty one months in prison. These people not only aimed to cause distress to the victims, but also created the chances for others to become influenced into making future swatting situations.

There are many examples of swatting incidents in healthcare: St Claire HealthCare has been threatened by an individual seeking to shoot people on the campus grounds. There were also claims to have an IED detonated in the location that was sent via email. These threats have caused the hospital to interact with law enforcement agencies but has not led to apprehension of the perpetrator. St. Claire HealthCare established a stronger security presence and further precautions for the premises.

Another notable swatting occurrence happened in Northwestern Memorial Hospital, one of Chicago's biggest hospitals, after authorities have received an 'active intruder threat'. The call was placed through the police scanner audio that claimed there was an individual holding a nurse hostage in an elevator with a gun. Law enforcement consisting of the Chicago police SWAT team, and hospital security then conducted a sweep of the entire building and lockdown, and concluded that there was no active

threat being undergone. This halted all hospital operations and has caused fear to all residents of the campus. Gregory O' Laughlin, a visitor to visit a friend, stated that, "it's just very scary because you don't know what is going on" (Barnes, Small 2022). Another witness, a patient, recalled being left on the cardiology floor in the dark for hours.

An investigation of a bomb threat in Orange County was also being looked into as a possible swatting call at MemorialCare Saddleback Hospital. Deputies responded to a call estimated around 3 PM from an individual claiming to be at the hospital location with a bomb. Law enforcement was dispatched to secure the perimeters of the location and evacuate all patients and staff. It was then after the search that it was confirmed that the reported bomb threat was false and hospital functions continued once deemed safe.

Alberta Children's Hospital located in Canada was also at the forefront of swatting calls as the hospital was put on lockdown for around an hour after police received a report of an incident involving firearms. The facility was then secured and searched for any existing threat with roadways also being blocked off. All attempts of safety were conducted and it was determined that the report was fake by police and no arrests have been made so far. Similar incidents also occurred at the SickKids Hospital in Toronto and Edmonton's Stollery Hospitals to which the police speculated to be related to one another.

In addition, Medicine Hat Hospital experienced a swatting attempt that involved a twelve year old boy who is a resident in Airdrie. It was discovered in the investigation that a twelve year old boy was the apparent victim in the swatting attempt of this hospital. At about 9:15 PM on Tuesday, May 5th, a male from St. Louis, Missouri alerted the Medicine Hat Hospital of a post on a forum website, known as Reddit, that spoke of threats aimed towards the hospital. As a result, the location was then placed on a lockdown. After thorough examination of the threat, it was discovered that the twelve year old boy residing in Airdrie, had a relation to Medicine Hat Hospital. The boy was believed to be playing online video games with other players throughout North America. Video games are often a big contributor to swatting calls as it is more convenient for someone to commit behind a computer screen without becoming exposed. Similarly, Andrew Finch, a bystander, had also become a victim of swatting which stemmed from online gaming. An innocent father of two, in Wichita, Kansas, was caught up in a disagreement over a \$1.50 bet that was over a game of Call of Duty. The perpetrator, Tyler Barris, called authorities falsely reporting that he had killed his father and was holding the rest of his family hostage and was planning a homicide-suicide. Andrew Finch's address was given to law enforcement which had ended up in him losing his life because of an officer shooting him under the false notion that he was armed, when in fact, Andrew was checking on why his home was being raided. In this certain situation, one of the players had become angry and said they were going to "swat" the Airdrie boy they had lost to. Following this information, the police was able to trace the original swatting threat against Medicine Hat Hospital to an IP address located in Seattle, Washington and found that the Airdrie boy was a victim that was involved in the swatting threat and had no correlation to the incident itself.

Plainsboro Hospital also experienced a swatting incident at University Medical Center of Princeton. It was a Wednesday afternoon, when multiple law enforcement units were dispatched to investigate a suspicious report. Plainsboro police were alerted to a threat received by the State police around 5 PM. The threat was transmitted through an automated message derived from an unknown source, declaring that there were two men with firearms on the third floor of the facility and a third armed man in the parking lot of the premises. Investigations were completed that showed that there was no evidence of armed men or related suspicious activity in the hospital. Preventative actions were taken for the safety of the community as police were assigned at the Plainsboro Road entrances diverting visitors.

IMPACT ON HOSPITALS

Hospitals can suffer consequences as a result of false swatting reports. The allocation of resources and law enforcement can be disrupted when they are called to respond to false swatting reports, potentially causing damage that cannot be undone. Threats and calls being made towards hospitals that justify the need for a SWAT team being dispatched is a costly burden for all taxpayer money. Kevin Kolbye, a former FBI agent with expertise in swatting, estimates incidents have jumped from four hundred cases in 2011 to over a thousand in 2019 (Center for Technology and Society 2022). It is estimated that an emergency SWAT response call in the United States can cost from \$3,000 to \$15,000 per incident. That depends on which state the response is called in, the overtime pay needed for officers on the call, and what resources are needed in the response (Moore 2022). Furthermore, each swatting call costs taxpayers about \$10,000 which totals up to about \$240,000 per year for the nation. The cost of deployment of SWAT teams vary as different situations range from severity or to the location or time of day. Lieutenant Katrina Pruitt who has overlooked the budget of the base, discusses the assorted cost of working SWAT teams. She has stated that small operations would often cost her about \$1,040 an hour, and in many cases the average SWAT calls would last around three to four hours (Diaz 2014). The specific time of day or night and day of the week fluctuates the cost as well. Much of the overtime pay for SWAT teams are done if the call is not within their usual regular business hours.

SWAT commanders also inform Action News of the average number of incidents that called for SWAT teams a year and the cost to do so. The commanders have said they usually respond to twenty four incidents per year which are estimated to be about \$300,000 for SWAT standoffs (Simms 2012). False swatting reports have unnecessarily consumed taxpayer dollars and limited resources. There have been many instances in which significant amounts of money have been lost. Following a swatting in Rochester, New York, Lieutenant Aaron Springer estimated the incident cost at up to \$15,000. In Denver, a 2015 swatting cost law enforcement \$25,000, while an incident in Long Beach, New York is estimated to have cost \$100,000 in 2014 (Center for Technology and Society 2022). Resources such as transportation, firearms consistently have to be directed and maintained through costs, so they will be able to perform efficiently in possible situations. The units carry seventy five pounds of gear every time they are out

on an operation (Diaz 2014). The time and resources that could have been spent on real emergencies are wasted when responding to false reports.

Swatting incidents have demonstrated that there is an apparent physical and emotional trauma to not only the victims but also the bystanders. Unfortunately, in most cases of swatting, victims have succumbed to injuries, or even death. SWAT teams that swarm a victim's living quarters can cause heart attacks, which can put their life at risk. There were many instances where the victims felt as though they were going to die. There are many accounts of wrongful deaths that have stemmed from law enforcement. Though physical injuries are what is often thought of as a result of swatting, emotional injuries are important to consider to all those involved. Victims of swatting often exhibit post-symptoms of emotional trauma including depression, suicidal tendencies, PTSD (post traumatic stress disorder), nightmares, etc. In scenarios where firearms are present, victims begin to feel fearful of the consequences of swatting which could result in wrongful deaths. Lee County Undersheriff Carmine Marceno described how a situation of swatting can worsen because of the element of people being inside a home and having no idea why they are being swarmed by law enforcement. "Think about how alarming it is to them, to find their house surrounded by police... to hear the deputy sheriffs... K9... hear the helicopter in the air" (Cifatte 2017).

Victims of swatting are not only impacted, but the hospitals also. Swatting calls directed towards hospitals are likely to have their reputation be at risk. Residents who have seen or heard news of a swatting in a hospital are prone to becoming more cautious of their safety. Patients may feel that there still needs to be improvements within the security of the hospital. In addition, hospitals who have previously gone through swatting can also cause patients to have distrust towards how effective the security is. Overall, the strength of the security may be thought of as not being adequately effective and a lack of attention to the well being of the residents.

STAFF TRAINING

Healthcare organizations must be able to respond to swatting incidents and reassess safety strategies to reduce harm. There are several steps that can be taken for these specific situations. In-service training can be conducted to help healthcare professionals and staff learn how to handle swatting incidents. Also being aware of the indicators of a false report, such as a call being directed to a non-emergency number instead of 911 can lead to combatting a swatting call (Moore 11). The New Jersey Cybersecurity and Communications Integration Cell presents other notable indicators of swatting. Those can be that the caller's tone and background noise does not match with the alleged emergency, the caller is unable to cooperate with the dispatcher in answering follow up questions (full name, phone number, current location), the caller being heard typing or clicking to search for information, the story of the caller changing over the course of the questioning, mispronunciation of the region such as the city, street, and building names, and much more (NJCCIC 2). Identifying the possible indicators of swatting and thoroughly assessing the situation can substantially mitigate the chances of a swatting call magnifying.

Reacting to swatting calls can determine the potential severity of the situation, but how the situation is handled after is just as important. Reactions during the call should not make the caller feel enabled to have the upper hand in the emergency. Dispatchers should be trained on how to handle calls appropriately and gather all necessary information. Information that can be of great assistance on tracking down the call include the exact time and date of the call, victim telephone number, the telecommunications provider, the incoming telephone number, detailed narration of the threat and description of caller (NJCCIC 4). Providing accurate information gives a clearer understanding of the predicament and how to address it. Responding to the swatting call should prioritize the security of the organization. Law enforcement should consider that there may be victims involved and that firearms should not always be used in situations where there can be fatal outcomes.

Telecommunications can be used effectively to counter swatting calls.

Telecommunications are a principal tool in improving information sharing to dispatchers and law enforcement. For example, the Seattle Police Department uses Rave Facility to store and share information about previous swatting incidents or threats. 911 operators are able to simultaneously dispatch emergency response teams and check the database to see if there has been a history of swatting calls directed to the location (Center for Technology and Society 2022). This telecommunication device assists to provide responders with information that should be considered before entering a potentially dangerous situation. This police department also has developed a registry to which individuals are able to register under to avoid unnecessary police responses if they feel as though they can be a target to these types of calls. In some cases, swatting calls have been determined to be false after police contact the landline or home owner's phone to verify everything is safe (Moore 11). All staff should be trained on observing their surroundings and take note of behaviors perceived to be suspicious or capable of causing danger and have to contact the authorities. Having emergency plans in place for staff and patients to follow in the event of swatting helps to keep everyone safe.

Efficient reporting of swatting incidents or attempts is critical. Without proper reporting of swatting calls, there is no background information that can be given that can lead to decision making of whether these calls are genuine and how to pinpoint the victims. Properly dispatching law enforcement can impact the outcome of these swatting calls and the damage caused. Hospital security should receive training regarding swatting. It is important for hospital security to be trained in safety protocols in order to maintain safety and be of assistance to law enforcement. De-escalation tactics are an essential part of reducing the severity of swatting calls. It is recommended to use a team approach, taking into account officer training and skill level, the number of officers, and whether any officer has established rapport with the subject (Seattle Police Department Manual 2021). De-escalation tactics can be beneficial in hospitals to help prevent potentially harmful situations without putting patients and staff at risk. Since high-priority incidents are less common in hospitals, it is useful to have established training and processes in place to ensure successful outcomes (Vince 2022). In relation to swatting calls being dispatched to hospitals, security should be thoroughly educated on how to


handle these calls, how to record important information, provide details to the appropriate law enforcement unit, and assist in protecting the hospital staff and patients.

LEGISLATION

Threats are not limited to a single degree of harassment, but rather impose two meanings. A true threat is defined as, “an intentional statement that expresses sincere intent to commit an act of unlawful violence against a particular individual or group” (Jaffe 475). A basic threat, on the other hand, “is a communicated intent to inflict harm or loss” (Jaffe 476). Basic threats often present a lower intent to cause harm as true threats. Legal statutes cover a broad range of the contents of a threat, but there still remains vagueness on the constituents of these factors. Swatting has been recognized as an act of online deviance since at least 2008 when the Federal Bureau of Investigation issued a memorandum to police forces across the USA warning of the rising trend of these crimes (Lamb 80). Despite the attempt of distributing the knowledge of swatting, some states and law enforcement have not made any existing movements against swattings or have not obtained the legislation to do so. Currently, there are no federal laws directed towards persecuting events related to swatting. Senator Charles Schumer introduced the Senate Bill of 2015 which stated, “any false, fictitious, or fraudulent statement... to a Federal law enforcement agency that causes an emergency Federal law enforcement response, the term of imprisonment shall be not more than 8 years” (Jaffe 467). Furthermore, the perpetrator would be fined upwards of \$10,000 for any resources that have been lost.

The Interstate Swatting Hoax Act, introduced in December of 2015, was created by Representative Katherine Clark, The bill made four alternatives for criminal sanctions. Depending on the result of the swatting: (1) if there is an emergency response, the person swatter can be fined, imprisoned for up to five years, or both; (2) if the swatting results in serious bodily injury, then the swatter can be fined, imprisoned for up to 20 years, or both; (3) if the swatting results in a death, then the swatter can be fined, imprisoned for up to life, or both; and (4) for any other result, the swatter can be fined, imprisoned for up to a year, or both (Jaffe 468). Within the New Jersey state, Assemblyman Paul D. Moriarty proposed the Act A3877, on November 13, 2014, which made violators face up to five to ten years in prison, and a fine up to \$150,000 for committing acts of swatting (Jaffe 468).

There is ongoing debate over the legislation regarding the actions that can be taken against swatting calls. The legal system struggles in categories of swatting and many perpetrators have not been apprehended or punished for their actions. There are many complexities that have to be addressed, such as the degrees of swatting. These degrees may range from swatting that: (1) results in death, (2) results in injury, and (3) is peacefully diffused (Mery 34). In situations where doxxing have been committed to expedite the events of swatting, there are also degrees consisting of (1) results in death, (2) results in injury, or (3) results in the unauthorized revelation of personally identifiable information that exposes the target to risk of physical danger (Mery 34). Law reform needs to be considered as a method to combat swatting violators. Professor Neal



Katyal stated, “the law hasn’t totally caught up to this type of thing” (Mery 33). As there are present cases of swatting occurring, there is no form of justice being done through penalties to relieve the suffering of the victims.

CONCLUSION

Swatting is likely to continue within the healthcare sector. Security professionals need to implement safety measures and be supported by policies provided by the organization. Healthcare facilities must be aware of the potential of swatting and how to identify and react to a swatting event. Healthcare facilities must have emergency response procedures in place to deal with the multiple scenarios (bomb threats, armed intruders, fire, etc.) that can be falsely reported.

AUTHOR

Nikki Le received a Bachelor of Science degree in Public Health from Stockton University in 2022. Her recent professional background involved interning at Virtua Health in security and safety. Nikki's research interest focuses on the relationship between technology and security, especially in devising approaches to fortify safety and security measures. Nikki aims to utilize her sustained interest in this field to facilitate efforts aimed at improving the security of the general public.

REFERENCES

- Allison, L. *Airdrie preteen victim of "swatting" attempt involving Medicine Hat Hospital*. DiscoverAirdrie. (2020, May 6). Retrieved January 6, 2023, from <https://www.discoverairdrie.com/articles/airdrie-preteen-victim-of-swatting-attempt-involving-medicine-hat-hospital>
- Burgess, K. 'Swatting' is 'a potentially deadly crime' that's very common. Police1. (2017, December 30). Retrieved January 6, 2023, from <https://www.police1.com/officer-shootings/articles/swatting-is-a-potentially-deadly-crime-thats-very-common-M7r3qVw3iX5OQubi/>
- Carrico, L. (2018). *Abstract assassination: How police militarization has contributed to the rise of "swatting"*. Encompass. Retrieved January 6, 2023, from https://encompass.eku.edu/honors_theses/596/
- Center for Technology and Society. *What is swatting?* ADL. (2017, July 3). Retrieved January 6, 2023, from <https://www.adl.org/resources/blog/what-swatting>
- Clark, J., Jackson, M., Schaefer, P., Sharpe, E. *Training Swat teams: Implications for improving tactical units*. Journal of Criminal Justice. Retrieved January 6, 2023, from https://www.sciencedirect.com/science/article/abs/pii/S0047235200000556?casa_token=pnbVekJW9I0AAAAA%3ASV4Tlc2t7R8_JlzMB78ydyLPS7lwHbsd4TBza6pYMUIM_46EMr-FxU_NPSIIK4t6WUOWYAP87tI
- Collins, George. (2022, September 6). *Swatting: A deadly twenty-first century prank*. South Seattle Emerald. Retrieved January 6, 2023, from <https://southseattleemerald.com/2020/01/09/swatting-a-deadly-twenty-first-century-prank/>
- Diaz, J. (2014, August 5). *How much it costs Austin every time SWAT teams roll out*. KUT Radio, Austin's NPR Station. Retrieved January 6, 2023, from <https://www.kut.org/crime-justice/2014-08-04/how-much-it-costs-austin-every-time-swat-teams-roll-out>
- FBI. (2013, September 3). *The crime of 'swatting': Fake 9-1-1 calls have real consequences*. FBI. Retrieved January 6, 2023, from <https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences1>
- FOX 11 Digital Team. (2021, December 27). *Authorities investigating bomb threat at hospital in Orange County as possible swatting call*. FOX 11 Los Angeles. Retrieved January 6, 2023, from <https://www.foxla.com/news/swatting-call-bomb-threat-saddleback-hospital>

- Jaffe, E. (n.d.). *Swatting: The New Frontier After Elonis v. United States*. Retrieved January 6, 2023, from <https://lawreviewdrake.files.wordpress.com/2016/08/jaffe-final.pdf>
- Lamb, J. B. (2020, July 3). *Death by Swat: The three elements of swatting*. Death by Swat: The Three Elements of Swatting | Emerald Insight. Retrieved January 6, 2023, from <https://www.emerald.com/insight/content/doi/10.1108/978-1-83867-447-220201005/full/html>
- Mery, H. (2021, October 29). *The dangers of doxing and swatting: Why Texas should criminalize these malicious forms of Cyberharassment*. Digital Commons at St. Mary's University. Retrieved January 6, 2023, from <https://commons.stmarytx.edu/thestmaryslawjournal/vol52/iss3/8>
- Moore, J. (2020). *Swatting: Tools for Detecting a Deadly Linguistic Prank*. ProQuest. Retrieved January 6, 2023, from <https://www.proquest.com/docview/2451351970?pq-origsite=gscholar&fromopenview=true>
- Moore, T.M. (2022, October 26). *What is swatting and how do you avoid becoming a victim?* VPNoverview.com. Retrieved January 6, 2023, from <https://vpnoverview.com/internet-safety/cybercrime/what-is-swatting/>
- Mustafa, H., Sadeghi, A.-R., Xu, W., & Schulz, S. (n.d.). *End-to-End Detection of Caller ID Spoofing Attacks*. Retrieved January 6, 2023, from <https://ieeexplore.ieee.org/ielaam/8858/8356073/7491306-aam.pdf>
- Nellist, A. (2018). *Swatting: Protecting the Individual*. ProQuest. Retrieved January 6, 2023, from <https://www.proquest.com/openview/f2007351c4896c72d4613799dae6a4b2/1?cbl=18750&pq-origsite=gscholar>
- NJCCIC. *Swatting MITGATION strategies and reporting procedures*. (n.d.). Retrieved January 6, 2023, from https://rems.ed.gov/docs/WA_Swatting.pdf
- Pavlicek, A., & Sudzina, F. (2018). *Internet security and privacy in VPN - dline.info*. Retrieved January 6, 2023, from https://www.dline.info/jnt/fulltext/v9n4/jntv9n4_1.pdf
- Perlman, M. (2022, April 26). *Sources say purported hostage situation that put Northwestern Memorial Hospital on lockdown was a hoax; not clear if it was a swatting incident*. CBS News. Retrieved January 6, 2023, from <https://www.cbsnews.com/chicago/news/sources-purported-hostage-situation-that-northwestern-memorial-hospital-lockdown-hoax/>

- Reed, T. (2018, October 3). *'Swatting' and other cyberthreats a growing problem for 911 call centers*. Fierce Healthcare. Retrieved January 6, 2023, from <https://www.fiercehealthcare.com/hospitals-health-systems/emergency-911-centers-need-more-funding-to-fight-back-against-cyber>
- Rosen, K. (2022, April 20). *Rowan county sheriff's office investigating 'swatting' incident at Morehead State, St. Claire Healthcare*. LEX 18 News - Lexington, KY (WLEX). Retrieved January 6, 2023, from <https://www.lex18.com/news/crime/rowan-county-sheriffs-office-investigating-swatting-incident-at-morehead-state-st-claire-hospital>
- Schmidt, C. (2018, February 27). *Alberta Children's Hospital locked down after police respond to swatting incident*. Calgary. Retrieved January 6, 2023, from <https://calgary.ctvnews.ca/alberta-children-s-hospital-locked-down-after-police-respond-to-swatting-incident-1.3818984>
- Seattle Police Department. *8.100 - De-Escalation - Police Manual*. (2021, April 15). Retrieved January 6, 2023, from <https://www.seattle.gov/police-manual/title-8---use-of-force/8100---de-escalation>
- Shaw, D. (2017, November 22). *'swatting' hoax can be costly to taxpayers*. WINK NEWS. Retrieved January 6, 2023, from <https://www.winknews.com/2017/11/21/swatting-hoax-can-costly-taxpayers/>
- Shea, K. (2015, May 27). *No threat found at Plainsboro Hospital placed on Lock Down*. nj. Retrieved January 6, 2023, from https://www.nj.com/middlesex/2015/05/plainsboro_police_place_hospital_on_lock_down.html
- Simms, R. (2012, January 3). *SWAT team incidents cost taxpayers \$300,000 each year*. KEPR. Retrieved January 6, 2023, from <https://keprtv.com/news/local/swat-team-incident-cost-taxpayers-300000-each-year>
- Vince, J. *No joke: Searching for serious solutions to 'swatting.'* Officer.com. (2022, September 26). Retrieved January 6, 2023, from <https://www.officer.com/tactical/swat/article/21274013/no-joke>