Catholic University Journal of Law and Technology

Volume 29
Issue 1 *Fall 2020*

Article 6

2020

The Survival of Critical Infrastructure: How Do We Stop Ransomware Attacks on Hospitals?

Helena Roland
Catholic University of America (Student)

Recommended Citation
Helena Roland, *The Survival of Critical Infrastructure: How Do We Stop Ransomware Attacks on Hospitals?*, 29 Cath. U. J. L. & Tech 177 (2020).
Available at: https://scholarship.law.edu/jlt/vol29/iss1/6

THE SURVIVAL OF CRITICAL INFRASTRUCTURE: HOW DO WE STOP RANSOMWARE ATTACKS ON HOSPITALS?

*Helena Roland**

In March 2018, a ransomware attack struck hospitals in Georgia, holding 3,789 computers hostage for ten days.[1] In September 2019, a ransomware attack cancelled numerous surgeries in Wyoming.[2] Since 2019, there have been 621 ransomware attacks on hospitals across the globe.[3] Malicious software has silently struck the nation's healthcare system at a dramatic pace, and there is no clear way to stop it. A place in which humanity seeks help and recovery is under attack and the attackers are not held accountable in a court of law.

Hospitals are a critical component of the nation's social infrastructure.[4] Take a moment: is it possible to name a person that has not sought out medical treatment? Additionally, is there a time when a patient walks into a medical facility and is able to withhold all personal information and data? The healthcare industry is rapidly growing, as necessary, to meet all needs. However, as the industry grows, so does the opportunity to strike.[5] Hospitals have access to social

* *Juris Doctor* Candidate, Columbus School of Law; *The Catholic University Journal of Law and Technology*, Production Editor, 2020–21; Bachelor of Arts in Political Science, Union College, 2018. Thank you to my wonderful parents, both of whom are physicians, who tirelessly fought to keep Americans safe throughout the COVID-19 pandemic.

[1] Vanessa Romo, *Georgia Charges Iranians in Ransomware Attack on Atlanta*, NPR (Dec. 5, 2018), https://www.npr.org/2018/12/05/673958138/georgia-charges-iranians-in-ransomware-attack-on-atlanta.

[2] Aimee Picchi, *Ransomware's Mounting Toll: Delayed Surgeries and School Closures*, CBS NEWS (Oct. 1, 2019), https://www.cbsnews.com/news/ransomware-attack-621-hospitals-cities-and-schools-hit-so-far-in-2019/.

[3] Picchi, *supra* note 2.

[4] *See* Ryan Nunn et al., *A Dozen Facts About the Economics of the US Health-Care System*, BROOKINGS (Mar. 10, 2020), https://www.brookings.edu/research/a-dozen-facts-about-the-economics-of-the-u-s-health-care-system/ (noting that the United States relies heavily on hospitals for employment and economic infrastructure).

[5] *See generally* Sylvestre Uwizeyemungu & Placide Poba-Nzaou, *Security and Privacy*

security numbers, bank account information, health records, familial background information, genetic information, and almost everything one would want to remain private in one's life.[6] Every time a patient walks into a doctor's office she must either fill out a form that has all personal data or she must check over that sheet to ensure that the data is correct. What would happen if unscrupulous individuals stole that information and held it for ransom?

This article will begin with the origins of ransomware attacks in 1989.[7] Then, it will discuss the definition of ransomware and how the tactic has been viewed in the modern world.[8] After defining the term, the article will turn to the reasoning behind hospital ransomware attacks and why a critical feature of the nation's infrastructure is under attack.[9] Consequently, there are practical and legal ramifications of ransomware attacks that must be addressed.[10] Finally, this article will look at how ransomware attacks can be deterred through the American legal system, such as the adoption of a criminal theory of general

Practice in Healthcare Information Systems: A Cluster Analysis of European Hospitals, *in* PROCEEDINGS OF THE 2ND INT'L CONF. ON INFO. SYS. SEC. AND PRIVACY 1, 41–44 (2016) (showing that as a hospital's reliance on technology increases, the need for secure IT protection increases).

[6] *See Patient Registration Forms*, DOCTORS CARE, https://doctorscare.com/patientforms/ (last visited Mar. 4, 2021); *see also New Patient Information and Consent*, DOCTORS CARE, https://doctorscare.com/wp-content/uploads/2019/11/PAT-F002A-11-19-DC-Patient-Information-and-Consent-New-Patient.pdf (last visited Mar. 4, 2021) (providing an example of the type of information that healthcare providers require from patients, including birthdate, social security number, address, and employer).

[7] Kaveh Waddell, *The Computer Virus That Haunted Early AIDS Researchers: The First-Ever Ransomware Attack Was Delivered on a Floppy Disk*, THE ATLANTIC (May 10, 2016), https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

[8] *Ransomware*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, https://www.us-cert.gov/Ransomware (last visited Mar. 4, 2021).

[9] Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*, 40 SEATTLE U. L. REV. 937, 941 (2017); *Hackers Demand $14 Million from Nursing Homes in Ransomware Attack*, CBS NEWS (Nov. 25, 2019), https://www.cbsnews.com/news/hackers-ransomware-nursing-homes-14-million/.

[10] *See* Manny Fernandez et al., *Ransomware Attacks are Testing Resolve of Cities Across America*, N.Y. TIMES (Aug. 22, 2019), https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html; *see also* Michael Balsamo, *2 Iranian Hackers Charged in Ransomware Scheme that Targeted Maryland's MedStar Health*, BALT. SUN (Nov. 29, 2018), https://www.baltimoresun.com/news/crime/bs-md-medstar-ransomware-indictment-20181129-story.html; *see also Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, U.S. ATT'Y OFF., N.D. OF GA. (Dec. 5, 2019), https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack.

deterrence,[11] creation of an American tribunal for cybercrime,[12] an implementation of cybercrime laws at local levels,[13] and an increase in federal funding.[14] This article will make it apparent that there is more the United States can do to prevent ransomware attacks.

I. ORIGINS OF RANSOMWARE ATTACKS

In 1989, the AIDS epidemic was at an all-time high: over 100,000 reported cases.[15] In the same year, the first major ransomware threat emerged entitled "AIDS Trojan."[16] An evolutionary biologist, Joseph Popp, created a computer-based questionnaire that helped patients determine the risk they had of contracting AIDS.[17] A disc was sent via mail entitled "AIDS Information Introductory Diskette," disguised as legitimate software on the AIDS epidemic to deceive recipients;[18] approximately 20,000 copies were distributed to 90 different countries.[19] After inserting the disc, nothing appeared different; however, ninety reboots later, the ransomware within the disc-delivered encrypted files, compromising the user's computer.[20] Victims' computers were frozen and could not be unlocked without a "licensing fee" paid to the hacker, which rendered most computers unusable.[21] The fee had to be paid either through a cashier's check or international money order.[22] Fortunately, researchers produced "antidotes" to record all files that were locked on victims'

[11] Robert Staal, *International Conflict of Laws — The Protective Principle in Extraterritorial Criminal Jurisdiction*, 15 U. MIAMI L. REV. 428, 428 (1961); Mark A. Drumbl, *Toward a Criminology of International Crime*, 19 OHIO STATE J. ON DISP. RES. 263, 264–82 (2003); Isak Ladegaard, *We Know Where You Are, What You Are Doing and We Will Catch You: Testing Deterrence Theory in Digital Drug Markets*, 58 BRIT. J. CRIMINOL., 414, 415 (2017).

[12] U.S. CONST. art. I, § 8, cl. 9; *see also* Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE J. INTL. L. 191, 223–26 (2018) ("The availability of an international criminal tribunal . . . would medicated many of the problems of State jurisdiction . . .").

[13] Alan Neuhauser, *Can the Law Stop Ransomware?*, U.S. NEWS (Apr. 13, 2019), https://www.usnews.com/news/national-news/articles/2018-04-13/can-the-law-stop-ransomware.

[14] Maggie Miller, *Lawmakers Criticize Trump's Slashed Budget for Key Federal Cyber Agenda*, THE HILL (Mar. 11, 2020), https://thehill.com/policy/cybersecurity/487120-lawmakers-criticize-trumps-slashed-budget-for-key-federal-cyber-agency.

[15] Waddell, *supra* note 7.

[16] Alexandre Gazet, *Comparative Analysis of Various Ransomware Virii*, 6 J. COMP. VIROL. 77, 78 (2010).

[17] Waddell, *supra* note 7.

[18] Gazet, *supra* note 16.

[19] Waddell, *supra* note 7.

[20] Gazet, *supra* note 16.

[21] Waddell, *supra* note 7.

[22] *Id.*

computers.[23] After Popp was arrested, it was discovered that the ransomware attack was a reaction to not being hired by the World Health Organization.[24] Popp was angry he was overlooked for a promotion and launched an attack on almost 100,000 people across the globe.[25] Ever since, the trend of ransomware attacks has been on the rise, with different motives behind each attack.[26]

II. WHAT IS RANSOMWARE?

The Cybersecurity and Infrastructure Security Agency ("CISA"), an agency within the Department of Homeland Security ("DHS"), defines "ransomware" as a type of malicious software ("malware") that is designed to restrict or deny access to computer data until a ransom, typically in the form of bitcoin, is fully paid by the victim(s).[27] More commonly, the definition of "ransomware" is malware that locks an individual's or company's computer, or the overall computer system, and prevents the individual or company from accessing the data until the affected party pays a ransom, usually in bitcoin.[28] Bitcoin is a method of "electronic cash" that is maintained through transactions with other users.[29] The malware enters the computer through three distinct methods: (1) through phishing emails, which is an email used by scammers to trick the receiving party into giving up personal information;[30] (2) through phishing emails that are sent from a company a party may know in an attempt to get the reader to click a link which releases the malware;[31] or (3) through "infected" websites that humans unknowingly visit.[32] Ransomware occurs in three phases: (1) seeking a target, (2) extortion and loss of access, and (3) ransom message display.[33] In the first phase, attackers target documents as it is quicker and more efficient to access information, and they eventually gain power over his or her

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *See id.* (noting that ransomware today is used to target incompetent technology users by convincing them something is horribly with their computers that can be fixed for a small sum, as well as to target hospitals with advanced encryption technology for ransoms as high as $17,000).

[27] *Ransomware*, *supra* note 8.

[28] Farringer, *supra* note 9, at 953.

[29] *What Is Bitcoin?*, BITCOIN MAG., https://bitcoinmagazine.com/guides/what-bitcoin (last visited Mar. 4, 2021).

[30] *How to Recognize and Avoid Phishing Scams*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (last visited Mar. 4, 2021).

[31] *Id.*

[32] *Ransomware*, *supra* note 8.

[33] Gazet, *supra* note 16, at 77–78.

victim(s) through freezing and extorting data.[34] Finally, the attacker reaches the ultimate goal of gaining money from the victim(s).[35]

Studies have found that hackers "exploit cyber weaknesses and gain access into victims' computers" to install the ransomware software remotely, then encrypt the files, freeze their entire computer, and demand payment in ransom to have the data unlocked.[36]

III. WHAT ARE HOSPITAL RANSOMWARE ATTACKS?

Ransomware attacks on hospitals are on the rise as hospitals are becoming uniquely vulnerable in the new digital age.[37] This vulnerability stems from (1) glacial-slow movement toward electronic medical records; (2) the Department of Health and Human Services' ("HHS") lack of enforcement of the Health Insurance Portability and Accountability Act of 1996 ("HIPPA"), and the Health Information Technology for Economic and Clinic Health Act ("HITCH") "with respect to security of electronic data;"[38] and (3) the sheer necessity of paying hackers for electronic data.[39]

First, massive computer systems are needed to transfer all medical data that was once recorded on paper to an electronic system, which opens a door for attackers to infiltrate the process of transferring data.[40] Expensive machinery is needed to sustain these massive electronic systems, which cost the hospital thousands if not millions of dollars. Thus, hospital executives are wary to spend even more money on security.[41] From stealing hospital-issued laptops or cell phones, to infiltrating large-scale HIPPA breaches, the sheer size of hospitals makes them accessible targets for attacks.[42] Furthermore, human error is a massive risk when it comes to ransomware attacks, and hospitals employ one of the largest networks of employees in the working world, from doctors to nurses to administrative staff.[43]

There is an immense financial incentive to attack hospitals because the

[34] *Id.*

[35] *Id.* at 78.

[36] Balsamo, *supra* note 10.

[37] Farringer, *supra* note 9, at 940–41.

[38] *Id.* at 941.

[39] *Hackers Demand $14 Million*, *supra* note 9.

[40] Farringer, *supra* note 9, at 956–57 (outlining generally the large-scale investments in IT security by many health institutions required to defend against ransomware attacks).

[41] *Id.* at 956–57 (outlining criticisms of the current IT security practices of many hospitals).

[42] *See id.* at 951 (noting that more recent data breaches have seen smaller breaches morph "into larger-scale HIPAA breaches, such as hackers infiltrating the networks of large health systems and insurers).

[43] *Id.* at 957.

attacker can demand more money due to the sensitive data and functionalities that live within hospital computers.[44] Mike Christman, a section chief for the cyber division of the Federal Bureau of Investigation ("FBI"), stated that "cybercrooks" know that hospitals "are more likely to pay if only because they can't afford not to."[45] The average digital extortion payout in 2018 was approximately $36,295.[46] Hospitals hit with ransomware attacks face the dilemma of paying the attacker in an attempt to get private data back or refusing to pay and risk losing all data.[47] Consequently, hospitals are more likely to pay the ransom than attempt to recover the stolen data through other software means.[48]

The two specific types of ransomware that are used to attack hospitals are the "Locky virus" and "Samas virus."[49] The Locky virus begins its attack on hospitals through emails that are opened by unknowing individuals in the hospital.[50] Next, the malware that has been unknowingly installed by the hospital employee moves through the system.[51] As a result, the malware locks out all users until access is granted by the attackers and once they have received the bitcoin payment.[52] On the other hand, the Samas virus attacks through "vulnerabilities in web servers."[53] One example of a common web server vulnerability is called an "SQL injection" where the attacker can gain access to a computer's database and even "spoof a user's identity," leading to the destruction or alteration of data within the database.[54]

IV. PREVIOUS RANSOMWARE ATTACKS ON HOSPITALS AND MEDICAL FACILITIES

In September 2019, Campbell County Health in Wyoming was subject to a

[44] *See id.* at 952 (noting the primarily financial motivations of many recent ransomware attacks on hospitals, as personal information can be sold as "hacked" data on the black market).

[45] *Hackers Demand $14 Million*, *supra* note 9.

[46] Picchi, *supra* note 2.

[47] *Id.*

[48] *Id.*

[49] Farringer, *supra* note 9, at 955.

[50] *Id*.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] Emily Pribanic, *Web Server Vulnerabilities Attacks: How to Protect Your Organization*, TECH FUNNEL (last updated June 29, 2020), https://www.techfunnel.com/information-technology/web-server-vulnerabilities-attacks-how-to-protect-your-organization/.

ransomware attack, which held all computers hostage.[55] As a result, surgeries were cancelled, laboratories and therapies were halted, the hospital would not take on new patients, and local community members were forced to travel to other hospitals.[56] Typically, smaller cities are more attractive targets for attackers because they lack resources to fight the attack and the money is coming from taxpayer dollars.[57]

On October 1, 2019, DCH Health System in Alabama had to close three separate hospitals to new patients because they were under ransomware attacks.[58] The hacker sent an email about the ransom information, alerting hospital staff of the impending attack.[59] The health network's computer systems were "paralyzed," and medical staff were forced to turn away "all but the most critical new patients."[60]As a result, ambulances were instructed to cease their usual activities—patrolling the streets to ensure proximity to potential health crises—to transfer all patients to other hospitals, thereby threatening the lives of patients who have to travel farther for healthcare.[61]

On September 30, 2019, seven Australian hospitals responded to a "cyber health incident."[62] A ransomware attack blocked access to several systems, including their financial management networks.[63] Consequently, hospital computer systems were locked for the first twenty-four hours after the attack.[64] Australian authorities stated that it would take weeks to secure and restore the damaged networks.[65]

On November 17, 2019, Virtual Care Provider, a company that provides technology to over one hundred nursing homes in the U.S., fell victim to a ransomware attack.[66] The hackers demanded fourteen million dollars before they would restore access to the company's servers.[67] The company was unable to pay the demand; consequently, many of the nursing homes that relied on the company were unable to access patient records, use the internet, order

[55] Picchi, *supra* note 2.

[56] *Id.*

[57] *Id.*

[58] Dan Goodin, *Ransomware Forces 3 Hospitals to Turn Away All but the Most Critical Patients*, ARS TECHNICA (Oct. 1, 2019), https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/.

[59] James Franklin, *DCH Health Systems Hit by Ransomware Attack, Not Taking Patients*, ABC 33/40 (Oct. 1, 2019), https://abc3340.com/news/local/dch-hospitals-hit-by-ransomware-attack-not-taking-patients.

[60] Goodin, *supra* note 58.

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Hackers Demand $14 Million*, *supra* note 9.

[67] *Id.*

medication, or pay their employees.[68] A day after the attack, the company learned that twenty percent of its services were affected and one hundred servers needed to be rebuilt.[69] After further investigation by a local security firm, it was determined that Russian hackers infected the company's computers over a fourteen-month timeframe using malicious email attachments.[70]

A. MedStar Health Attack – March 28, 2016, Maryland

On March 28, 2016, one of the most extensive ransomware attacks happened in Washington, D.C.[71] Employees at MedStar Health began to see pop-up messages on computer screens that were seeking payment in bitcoin for hijacked data: $19,000 in exchange for a digital key that would release all data.[72] All systems remained dark over a ten-day holdout period: ten hospitals and 250 outpatient centers had to shut down all computers.[73] Patients were either turned away or treated without proper computer records.[74]

Over 30,000 employees were forced to use old paper records to treat incoming and current patients, which led to a dangerous patient safety issue.[75] For example, the attack led to lab results taking much longer than usual, and it caused a nurse to accidentally continue a patient's powerful antibiotic treatment for eight hours longer than necessary.[76] Additionally, appointments were cancelled for non-life-threatening health issues, such as quarterly visits with kidney specialists and weekly radiation treatment.[77] The encrypted hospital data caused staff and patients "to report delays in service and confusion in treatment."[78]

This attack was, unfortunately, successful because of the specific tactics employed by the hackers. First, the hospitals were targeted after normal business hours, so there were few members on hand to respond to the immediate attack.[79] Second, the hackers used European-based services to launch the attacks on the

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] John Woodrow Cox, *MedStar Health Turns Away Patients After Likely Ransomware Cyberattack*, WASH. POST (Mar. 29, 2016), https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html.

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] Balsamo, *supra* note 10.

[79] *Id.*

hospitals from a remote location, which would later be determined as Iran.[80]

V. CONSEQUENCES OF RANSOMWARE ATTACKS

After the MedStar ransomware attack, the FBI and US Secret Service tracked the hackers to Iranian computers.[81] These hackers were found to have been at the helm of schemes targeting government agencies, small cities, and local businesses in the US.[82] In addition to targeting MedStar Health, these hackers attacked the cities of Atlanta, Georgia, and Newark, New Jersey; they attacked the Colorado Department of Transportation, the San Ysidro Port in San Diego, and five other healthcare companies in the US.[83] Overall, these hackers amassed almost $6 million, while their victims suffered more than $30 million in losses.[84]

The attack encrypted data from computers of more than 200 victims.[85] The attackers used "SamSam" ransomware,[86] a form of the Samas virus,[87] to attack each of the victims.[88] The financial recovery can cost upwards of millions of dollars, potentially running many smaller cities and governments into bankruptcy.[89] As a result of this vicious malware, "cyberinsurance" has been on the rise: an insurer will now pay the requested ransom to help limit the catastrophic results that stem from losing data.[90]

Cyber insurance is offered to organizations that use computer systems in their businesses.[91] This form of insurance can benefit the organization when it is facing a lawsuit from owners of data that has either been "lost or compromised by a hacker" from the organization's computer system.[92] Cyber insurance "covers financial losses that result from data breaches and other cyber events."[93] When it comes to "cyber extortion," also known as ransomware, cyber insurance

[80] *Id.*

[81] *Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, *supra* note 10.

[82] Balsamo, *supra* note 10.

[83] *Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, *supra* note 10; Balsamo, *supra* note 10.

[84] Balsamo, *supra* note 10.

[85] *Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, *supra* note 10.

[86] Balsamo, *supra* note 10.

[87] Farringer, *supra* note 9, at 955.

[88] Balsamo, *supra* note 10.

[89] *See* Fernandez et al., *supra* note 10.

[90] *Id.*

[91] Marianne Bonner, *What Does a Cyber Liability Policy Cover?*, BALANCE SMALL BUS. (Dec. 9, 2019), https://www.thebalancesmb.com/what-s-covered-under-a-cyber-liability-policy-462459.

[92] *Id.*

[93] *Id.*

typically extends to "any extortion payment" or expenses incurred in responding to the demand of the extorter.[94] According to Raytheon, an aerospace and defense company,[95] "97% of networks will experience a security compromise over any given six-month period;" therefore, cyber insurance is necessary to protect a company from vulnerability.[96] The cost of cyber insurance varies based on the size of the company, annual revenue, and the industry, but typical premiums can incur an annual cost of anywhere from $650 to $120,000.[97]

However, regardless of the growing cyber insurance industry, the ransomware business is so lucrative that hackers are putting profits made from the ransom into research on how to execute ransomware attacks more fluidly.[98] For example, in May 2017, the city of Baltimore was attacked by ransomware with the hacker's ultimate goal of $76,000 in bitcoin, or else the hacker would not release the city's files.[99] The city refused, and the resulting damage cost more than the original ransom: $5.3 million was spent on computers and contractors to recover the lost information; lost revenue and expenditures cost more than $18 million; and many of the city's residents faced water bills more than three times the normal amount.[100]

VI. LEGAL RAMIFICATIONS OF RANSOMWARE ATTACKS

As a result of this vicious malware, the FBI, US Secret Service,[101] National Security Agency ("NSA"), and other intelligence bodies have become increasingly involved in ransomware attacks.[102] Recent attackers have been both American-born as well as foreign nationals from Eastern Europe and Iran.[103] Craig Carpentino, the US Attorney for New Jersey, stated that not only were these attackers installing ransomware for money, but they were also "seeking to harm our institutions and our critical infrastructure."[104]

On a state level, states governments from California, Connecticut, Michigan,

[94] *Id.*

[95] *What We Do*, RAYTHEON, https://www.raytheon.com/capabilities (last visited Mar. 4, 2021).

[96] Brand Barney, *Cyber Breach Insurance: How Much Does It Cost?* SECURITYMETRICS, https://www.securitymetrics.com/blog/cyber-breach-insurance-how-much-does-it-cost (last visited Mar. 4, 2021).

[97] *Id.*

[98] Fernandez et al., *supra* note 10.

[99] *Id.*

[100] *Id.*

[101] *Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, *supra* note 10.

[102] Fernandez et al., *supra* note 10.

[103] *Id.*

[104] Balsamo, *supra* note 10.

Texas, and Wyoming have introduced new laws that specifically target "'ransomware' or computer extortion."[105] For example, Connecticut has a law that grants prosecutors the power to apply traditional extortion charges, as necessary, to ransomware attacks. These can result in three years imprisonment.[106]

The paramount example is a 2018 pending case in the US state of Georgia against two Iranian nationals, Faramarz Shahi Savandi and Mohammed Mehdi Shah Mansouri. The men deployed the attack on MedStar Health in the Washington, D.C., region and the attack against the city of Atlanta using the same "SamSam" ransomware.[107] The March 2018[108] attack focused on city computer systems and attempted to extort "tens of thousands of dollars" from the government of Atlanta.[109] The attack lasted longer than a week, with an original demand of $51,000 and 3,789 computers held hostage.[110] A federal grand jury indicted the two men in the US District Court for the Northern District of Georgia for violating the Computer Fraud and Abuse Act.[111]

Additionally, both men were indicted by a federal grand jury in New Jersey for six different counts of conspiracy, fraud, and intentional damage.[112] The two District Courts worked in coordination with one another and the Computer Crime and Intellectual Property Section of the United States Department of Justice.[113] In December 2015, the two men accessed computers of victims, hospitals, municipalities, and public institutions, and installed "SamSam" ransomware to encrypt data on their computers.[114] The indictment included victims across North America, from the cities of Atlanta and Newark to the University of Calgary in Alberta, Canada.[115] The indictment, "the first of its kind," outlined "an Iran-based international computer hacking and extortion scheme that engaged in 21st-century digital blackmail."[116] As promising as both

[105] Fernandez et al., *supra* note 10.

[106] *Id.*

[107] *Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, *supra* note 10.

[108] *Id.*

[109] Romo, *supra* note 1.

[110] *Id.*

[111] *Id.*

[112] *Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, *supra* note 10.

[113] *Id.*

[114] Office of Public Affairs, *Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses*, U.S. DEPT. OF JUST. (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[115] *Id.*

[116] *Id.*

indictments may sound, legal scholars have been wary to hold out hope for justice against Savandi and Mansouri: the US does not have an extradition treaty with Iran, so a trial likely cannot be held if both defendants are hiding abroad.[117] However, these indictments are part of a larger strategy of the US government in an attempt to create "legally admissible cases against foreign cyber attackers."[118] As of right now, attackers are "unlikely to see the inside of a [US] courtroom."[119]

VII. TRANSNATIONAL CYBERATTACKS – RANSOMWARE

Cyberspace is a term that is difficult to grasp; it has been deemed a space that "lacks geographic boundaries and does not map neatly onto the traditional system of territorial jurisdiction."[120] One major problem with cybercrimes is the issue of transnational cyber offenses and how a state may claim jurisdiction.[121] One of the most common types of transnational cyberattacks is infectious malware, the overarching category that encompasses ransomware.[122]

With cyberattacks becoming more frequent, the government needs to adjust its legal system to incorporate civilian and international attackers.[123] Currently, the FBI prosecutes computer crime and the Defense Department ("DoD") prosecutes cyberwarfare.[124] However, ransomware is a form of computer crime and, at the same time, cyberwarfare, as it seeks to extort its victims.[125] Which internal agency prosecutes the hackers? Domestic cybercrime laws traditionally do not extend extraterritorially as it is viewed as a violation of other nations' sovereignty.[126] Which country can prosecute the hackers? American cybercrime enforcement, especially relating to the healthcare industry, is very limited.[127] Therefore, the government must act before taxpayers lose more money, hospitals shut down, operating rooms go dark, and local governments go bankrupt by attempting to regain data.

[117] Romo, *supra* note 1.
[118] *Id.*
[119] *Id.*
[120] Perloff-Giles, *supra* note 12, at 192.
[121] *Id.*
[122] *Id.* at 197.
[123] *Id.* at 200.
[124] *Id.*
[125] *Id.*
[126] *Id.* at 206.
[127] John P. Mello, Jr., *Healthcare Security $65 Billion Market: Ransomware Attacks on Healthcare Organizations are Predicted to Quadruple by 2020,* CYBERCRIME MAG. (Apr. 6, 2017), https://cybersecurityventures.com/healthcare-cybersecurity-report-2017.

VIII. DISCUSSION

The paramount question facing our legal system is how our government can get international attackers on US soil to face their day in court for the attacks they executed against American victims? Cyberattacks on American hospitals are one of the few non-violent acts that can create a fine line between life and death; therefore, making a legal statement to ensure hackers do not continue to infiltrate our healthcare system is of the utmost importance.[128] I argue that the lack of procedural guidelines over how to prosecute ransomware hackers is putting American lives at risk. The US government needs to implement measures to specifically target international hospital hackers, or else private data could have the dangerous potential to go public with no way to stop it.

Before addressing ways to manage this new form of cyberattack, it is necessary to understand why stopping ransomware in the American healthcare system is imperative on a global level. Healthcare company data is extraordinarily valuable. It is a highly sought-after target for attackers: "You can do anything with a complete electronic health record."[129] Stephen Batchelder, the Massachusetts Interlocal Insurance Association's ("MIIA") Director of Claims and Risk Management Operations stated, "When critical systems at hospitals, police and fire departments, or vital infrastructure systems such as water, electricity, and natural gas are attacked, public safety and individual welfare can be put at risk."[130] An attack on a healthcare system is ultimately an attack on America's critical infrastructure.[131] Researchers at Vanderbilt University's Graduate School of Management analyzed an HHS list of more than 3,000 hospitals, about ten percent of which suffered from a data breach.[132] The study found that after data breaches, "as many as 36 additional deaths per 10,000 heart attacks occurred annually at the hundreds of hospitals examined."[133] Additionally, for healthcare centers that experienced a ransomware attack, it took an additional 2.7 minutes for patients suffering from a heart attack to receive an electrocardiogram,[134] a test used to detect heart

[128] Fred Donovan, *Defending Against Healthcare Ransomware Attacks*, HEALTH IT SEC. (May 4, 2018), https://healthitsecurity.com/features/defending-against-healthcare-ransomware-attacks.

[129] *Id.*

[130] Stephen Batchelder, *Local Governments Must Address Cybercrime Vulnerabilities*, MASS. INTERLOCAL INS. ASS'N., https://www.emiia.org/about/46/view-news-item (last visited Mar. 4, 2021).

[131] Perloff-Giles, *supra* note 12, at 203.

[132] Brian Krebs, *Study: Ransomware, Data Breaches at Hospitals Tied to Uptick in Fatal Heart Attacks*, KREBS ON SEC. (Nov. 7, 2019), https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks/.

[133] *Id.*

[134] *Id.*

problems.[135] Researchers from Vanderbilt also discovered that remediation efforts after a data breach were associated with a decline in the timeliness of care and patient outcomes.[136] The former Deputy Chief Information Security Officer at HHS, Leo Scanlon, stated that "the exploitation of cybersecurity vulnerabilities is killing people."[137] Overall, the study found that "hospitals that have been hit by a data breach or ransomware attack can expect to see an increase in death rate among heart patients in the following months or years because of cybersecurity remediation efforts."[138]

A. Measures to be Implemented – International & Domestic Jurisprudence

First and foremost, before implementing any other form of international jurisprudence toward healthcare ransomware prevention, the US must set forth a theory of protective extraterritorial jurisdiction over ransomware attacks on American healthcare systems. The protective theory claims jurisdiction over any act "predicated on the national interest injured by the offense committed abroad."[139] This theory, based on self-defense, was designed to protect the national interest of the injured country through its legal system.[140] The hacking of healthcare systems in the US is a matter of national security, as it is the nucleus of American infrastructure, which houses almost every single American's personal data and effects. Thus, if protective jurisdiction is ensured through international treaties, agreements, and statements by public officials, US courts would have the power to hear these cases without question.[141]

1. Criminal Theory of General Deterrence

A court system is built to ensure accountability of one's actions: "accountability is cast as a prerequisite for justice."[142] The main method of international criminal accountability is jail time.[143] Without accountability, our system would descend into chaos as criminals could escape without

[135] *Electrocardiogram (ECG or EKG)*, MAYO CLINIC, https://www.mayoclinic.org/tests-procedures/ekg/about/pac-20384983 (last visited Mar. 4, 2021).
[136] Krebs, *supra* note 132.
[137] *Id.*
[138] Krebs, *supra* note 132; Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERV. RES. 971 (2019).
[139] Staal, *supra* note 11, at 428.
[140] *Id.* at 429
[141] *See id.* at 428 (recounting a case where the U.S. had jurisdiction over a Mexican citizen because the crime affected U.S. sovereign territory).
[142] Drumbl, *supra* note 11, at 264.
[143] *Id.*

repercussions: "without accountability measures, cyberspace risks becoming a Hobbesian state of nature in which victims engage in self-help and cyber-vigilantism."[144] A government cannot allow victims to take accountability into their own hands. There must be legal measures in place to ensure the hackers will be brought to justice in a court of law. Currently, there are no accountability measures in place because the field of ransomware attacks is new and law enforcement officers, coupled with the judiciary, need a system in which to execute and enforce laws on a cyber-plane.

One measure that could be implemented is a form of international criminal jurisprudence through general deterrence as to healthcare ransomware. It is a well-known theory that if general deterrence triumphs, "crises and wars do not occur."[145] General deterrence addresses the assumption that human beings act based on what is in their best benefit.[146] Relatedly, human beings will aim to avoid "unpleasant consequences, such as punishment;"[147] therefore, if the punishment becomes more severe, the hacker is less likely to break the law, resulting in a decreased crime rate.[148] The key is "to install a sense of increased risk of punishment in the individual that is contemplating criminal behavior."[149] Although there is a growing trend that harsher punishment does not lead to an effective cease of criminal activity,[150] prevention coupled with accountability, in the form of general deterrence, can formulate a targeted international criminal justice campaign.[151]

The International Criminal Tribunals for the former Yugoslavia ("ICTY") and Rwanda ("ICTR") rationalized the punishment of crimes before these courts under each of the traditional justifications for punishment: retribution, deterrence, isolation, and rehabilitation.[152] In many imperative cases, the tribunals impose sentences with the goal of deterrence to warn future international leaders that "they will be held accountable for their behavior."[153] As stated above, ransomware in hospitals is some of the most destructive cyber-

[144] Perloff-Giles, *supra* note 12, at 192.

[145] Stephen L. Quackenbush, *General Deterrence and International Conflict: Testing Perfect Deterrence Theory*, 36 UNIV. OF MO. INT'L INTERACTIONS: EMPIRICAL AND THEORETICAL RES. IN INT'L REL. 60, 61 (2010).

[146] Ladegaard, *supra* note 11, at 414.

[147] *Id.* at 416

[148] *Id.* at 414.

[149] *Id.*

[150] *See* Kelli D. Tomlinson, *An Examination of Deterrence Theory: Where Do We Stand*, 80 FED. PROBATION 33, 34 (2016) (noting that recent literature suggests that harsher punishments either do not lower criminal activity, or that any lowering of criminal activity is due to more offenders being incapacitated instead of a general deterrence effect).

[151] Perloff-Giles, *supra* note 12, at 209.

[152] Andrew N. Keller, *Punishment for Violations of International Criminal Law: An Analysis of Sentencing at the ICTY and ICTR*, 12 IND. INT'L & COMP. L. REV. 53, 57 (2001).

[153] *Id.* at 61.

warfare to date. As such, it is in the interest of national security to put an end to it. Therefore, a strict punishment should be applied to perpetrators to deter copycats and likeminded individuals from attacking the data of US citizens.

2. US Tribunals for Cybercrime

The US government can ensure protection from international cybercrime in the form of hospital ransomware by the creation of a forum to hear civil cases stemming from cybercrime hackers.[154] During a criminal trial, or even after the case has ended, civil cases for economic damages allow the victims to receive some form of compensation. In the case of healthcare ransomware, civil cases can come from the hospitals attacked, the patients whose data was breached, or the local government who had to pay for the repercussions. These forums can take the form of Article I courts.[155] The Constitution enables Congress to create inferior tribunals to hear different matters.[156]

Precedent has been set for independent tribunals through *Dames & Moore v. Regan*.[157] In response to the seizure of the US Embassy in Tehran, Iran and its US occupants, President Jimmy Carter used the International Emergency Economic Powers Act ("IEEPA") to seize all Iranian property in the United States.[158] Consequently, Dames & Moore filed suit against the Government of Iran, the Atomic Energy Organization of Iran, and Iranian banks with allegations of money owed for services performed for the Atomic Energy Organization.[159] As a result, the district court issued orders of attachment against property of the co-defendants to secure a judgment.[160] Iran and the US came to an agreement on January 19, 1981, known as the Algiers Accords, which freed all US hostages in exchange for the termination of all legal proceedings against Iran in US courts and the nullification of judgments against the foreign state.[161] Dames & Moore filed suit against the US seeking to prevent the enforcement of the Accords, which nullified the claim against the Iranian co-defendants.[162]

[154] *See* Perloff-Giles, *supra* note 12, at 209–11 (noting that ensuring accountability and preventing victims from resorting to "cyber-vigilantism" includes providing a forum for businesses to bring complaints and seek some kind of relief).

[155] U.S. CONST. art. I, § 8, cl. 9.

[156] *Id.*

[157] Dames & Moore v. Regan, Secretary of Treasury, et al., 453 U.S. 654, 654 (1981).

[158] *Executive Power Under Dames & Moore v Regan*, CONST. L. REP., https://constitutionallawreporter.com/2019/04/25/dames-moore-v-regan-1981/, (last visited Mar. 4, 2021).

[159] *Id.*

[160] *Id.*

[161] *Id.*

[162] *Id.*

The case went up to the Supreme Court of the United States, which upheld the constitutionality of the Algiers Accord and the creation of the Iran-United States Claims Tribunal ("IUSCT") in response to the Iranian hostage crisis.[163] The IUSCT only hears commercial claims generated by the crisis between US nationals and Iran.[164] The tribunal was created through the use of IEEPA, an act of Congress, and the Algiers Accord, a treaty that was created by the President with the advice and consent of the Senate, making the IUSCT an Article I court.[165]

Another example of an Article I tribunal is the United States Tax Court ("Tax Court").[166] The Tax Court is implicated when the Commissioner of the Internal Revenue Service ("IRS") determines there is a tax deficiency.[167] Additionally, the United States Court of Appeals for Veterans Claims ("Veterans Claims Court") is another example of an Article I tribunal.[168] The Veterans Claims Court was established through the Veterans' Judicial Review Act, signed by President Ronald Reagan, which gave the court "exclusive jurisdiction over decisions of the Board of Veterans' Appeals."[169] Both courts, like the IUSCT, are authorized by Article I of the Constitution to hear cases and controversies as designated by Congress.[170]

A new cybercrime tribunal, established through Article I, would solely focus on civil claims from prosecutions against international hackers, thereby promoting a legal remedy for victims in court.[171] These tribunals create a new avenue through which ransomware hackers can be hauled into US courts: "the potential for individual victims to aggregate claims and obtain significant damages awards could meaningfully deter would-be cyber attackers."[172] If patients of a hospital that suffered from a ransomware attack accumulated all claims into one class action against the attacker, the resulting measures could be so severe that future hackers would be deterred from committing similar crimes. The knowledge of a hacker facing not only criminal penalties of potential jail time, but also civil penalties amounting to millions of dollars, could potentially

[163] Dames & Moore, 453 U.S. at 686.

[164] *Id.* at 684–87.

[165] U.S. CONST. art. I, § 8, cl. 9; CHRISTOPHER A. CASEY ET. AL., CONG. RESEARCH SERV., R45618, THE INT'L EMER. ECON. POWERS ACT: ORIGINS, EVOLUTION, AND USE 28 (2019).

[166] *Mission Statement*, U.S. TAX CT., https://www.ustaxcourt.gov/mission.html (last visited Mar. 4, 2021).

[167] *Starting a Case,* U.S. TAX CT., https://www.ustaxcourt.gov/petitioners_start.html (last visited Mar. 4, 2021).

[168] *About the Court,* CT. VET. APP., http://www.uscourts.cavc.gov/about.php (last visited Mar. 4, 2021).

[169] *Id.*

[170] U.S. CONST. art. I, § 8, cl. 9.

[171] Perloff-Giles, *supra* note 12, at 212–13.

[172] Perloff-Giles, *supra* note 12, at 214.

stymie future hackers from committing the same crimes.

For example, in the March 2016 MedStar Health ransomware attack, hundreds of potential patients were turned away because the computer software was completely frozen.[173] These turned-away patients could pursue a class action suit against the hacker for creating the chaos that led to hospital staff transferring them to other hospitals. Class action suits are time and cost efficient for the court system; thus, they are also beneficial to the government.[174] Class actions also have a higher likelihood of financial recovery, thereby if judgment is rendered against the defendant, he or she will most likely have to pay a large sum of money to all participants in the suit.[175] Therefore, if all victims ban together to file a claim against their ransomware attacker, the likelihood of a large financial judgment rendered in their favor is even higher. This assurance can also create a form of deterrence for future potential hackers.[176]

In the May 2017 Baltimore City attack, the local government paid over $18 million to restore the data lost by the ransomware attack.[177] From the $18 million, $5.3 million went to contractors to help restore lost data.[178] New domestic cybercrime tribunals, in the event of another Baltimore-type situation, could create an avenue in which Baltimore could seek restitution for the immense loss rather than leaving the crime unrectified, often resulting in higher taxes for residents and a loss of profits for the city as a whole.[179] The idea that a local government could bring an international hacker to court to seek restitution for immense damages to the hospital, its patients, or even the city, as a whole, could create less chaos and fear if another attack were to happen in the future.

Although Congressional action is needed in order to create a tribunal, the construction of a forum in which victims of cyberattacks can bring their attacker(s) to justice is one method in which the US government can pursue legal avenues of deterrence.[180]

3. International Tribunals

On an international level, the Security Council (Council) of the United

[173] Woodrow Cox, *supra* note 71.

[174] *What Are the Advantages of Joining a Class Action Lawsuit?*, THE MARGARIAN LAW FIRM (July 13, 2018), https://margarianlaw.com/joining-class-action-lawsuit/.

[175] *Id.*

[176] Perloff-Giles, *supra* note 12, at 214.

[177] Fernandez et al., *supra* note 10.

[178] *Id.*

[179] *See id*. (noting that residents were subject to water bills "three times as much as normal" following a ransomware attack).

[180] Perloff-Giles, *supra* note 12, at 214–15.

Nations (U.N.) has created several tribunals to hear specific categories of cases and controversies.[181] Chapter V of the U.N. Charter gives the Council power.[182] This power allows the Council to establish tribunals "to bring justice to victims of international crimes."[183] The Council created the ICTY, a tribunal responsible for prosecuting people who committed gross violations of human rights in the former territory of Yugoslavia.[184] Legal precedent for these tribunals established by the Council came from the trial of Duško Tadić.[185] The case addressed the question of whether the ICTY was legitimately formed through the U.N. Security Council.[186] The court determined that the ICTY was properly formed and had jurisdiction to hear all cases and controversies within the defined limits created by the Council.[187] This determination further establishes that a lawmaking body has the power to create and outline the powers of tribunals.

B. Measures to be Implemented – Adopt Cybercrime Law at Local Levels

On a much smaller scope than a reformation of international and domestic legal practices, local governments must adopt laws and regulations that outlaw cybercrime.[188] Information Security Media Group conducted a survey in 2014 that discovered "at least one security breach that affects fewer than 500 individuals has occurred in 75% of surveyed healthcare organizations."[189] Additionally, "at least one incident affecting more than 500 individuals has been reported by 21% of surveyed healthcare providers."[190] Another study projected over four million ransomware variants were detected in only the first quarter of 2015.[191] *Government Technology* described local government cybersecurity as a "crisis," with the probability of cyberattacks increasing in 2020.[192] The practice of ransomware is increasing on a global scale, and local governments

[181] *See UN Documentation: International Law*, DAG HAMMARSKJÖLD LIB., https://research.un.org/en/docs/law/courts (last visited Mar. 4, 2021).

[182] U.N. Charter art. 24, ¶ 1.

[183] *UN Documentation: International Law*, *supra* note 181.

[184] *Id.*

[185] Prosecutor v. Tadić, Case No. IT-94-1-T, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶¶ 70, 79, 137 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[186] *Id*. at ¶¶ 2, 9, 12, 13, 137.

[187] *Id.* at ¶¶ 22, 79, 137.

[188] Neuhauser, *supra* note 13.

[189] Uwizeyemungu & Poba-Nzaou, *supra* note 5.

[190] *Id.*

[191] Nikki Spence et al., *Ransomware in Healthcare Facilities: The Future is Now,* MARSHALL U. (2017).

[192] Dan Lohrmann, *How Local Governments Can Address Cybersecurity Challenges,* GOV'T TECH. (Aug. 4, 2019), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-local-governments-can-address-cybersecurity.html.

must act through legal means to curb the enticing reward that ransomware can provide.[193]

At the federal level, the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act criminalize illegal online activity, however, there is limited state law that criminalizes ransomware.[194] Almost every state has implemented computer crime laws and data-breach disclosure laws.[195] Only Connecticut, Texas, Wyoming, Michigan, and California have explicitly made ransomware a crime.[196] Wyoming law makes possession of ransomware, spyware, adware, keyloggers, and similar types of malware illegal.[197] Michigan law makes it illegal only if the perpetrator possesses ransomware software and intends to deploy it against another.[198] Both laws explicitly demonstrate that a state must be careful when outlining what makes ransomware illegal.[199] Additionally, if the law is defined as sheer possession of ransomware on an electronic device, victims would be at risk of violation as hackers infect their devices with ransomware: "if you get hacked, you're going to be in some form of possession of [malware.]"[200]

In 2018, 265 bills or resolutions affiliated with cybersecurity were considered by thirty-five states, along with D.C. and Puerto Rico.[201] The key areas of the bills include: augmenting government security practices, promoting training on cybersecurity, and providing funding for cybersecurity programs.[202] In 2019, the amount of states and US territories that have considered cybersecurity bills has increased to forty-three states and Puerto Rico.[203] Close to 300 bills were considered among the forty-three states and Puerto Rico, with thirty-one enacting cybersecurity-related legislation.[204] The topics are broadening to include: requiring agencies to train employees on security practices, creating task forces to combat cybercrimes, and addressing cybersecurity political

[193] *Id.*

[194] Neuhauser, *supra* note 13.

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *See* H.B. 5257, 99th Leg., Reg. Sess. (Mich. 2017); Neuhauser, *supra* note 13.

[199] Neuhauser, *supra* note 13.

[200] *Id.*

[201] *Cyber Security Legislation 2018*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 8, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx.

[202] *Id.*

[203] *Cyber Security Legislation 2019*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 10, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx.

[204] *Id.*

threats.[205]

In 2016, the University of Maryland, along with the International City/County Management Association, conducted a nation-wide survey on local government cybersecurity.[206] Approximately thirty-eight percent of local governments were found to be reliant on generationally inept technology.[207] Additionally, fewer than half of the local governments surveyed had bought cybersecurity insurance.[208] The FBI has repeatedly stated that a current, leading cyberthreat to local governments is ransomware.[209] For example, Fort Worth, Texas, is subject to 15,000 cyberattacks daily.[210] The responsibility of the cyber protection of constituents and local infrastructure belongs to "the entire chain of elected and appointed officials in local government."[211] The government cannot leave the duty of cybersecurity to the information technology departments of local businesses and hospitals. Local governments must step in and prevent future attacks.[212] Dr. Allan R. Shark, the executive director of the Public Technology Institute, emphasized that local governments should outsource all information technology: "Recent ransomware attacks have brought to light many deficiencies in digital hygiene . . . [g]iven the growing complexities of planning and maintaining technology as well as having the right staff, many local governments might be much better off outsourcing some or all of their IT operations."[213]

Although experts have stated that local governments need to start adopting policy to combat cyberattacks, there are many challenges that have stymied efforts.[214] Teri Takai, the executive director for the Center for Digital Government, outlined the challenges for local governments' cybersecurity efforts: lack of resources, antiquated technology, introduction of new technology, scope of local government, lack of funding in executive roles, and lack of understanding of cybersecurity issues.[215]

When it comes to critical state interests, such as elections, transportation, and intelligence, municipalities tend to collaborate with one another—sometimes across state lines—and with the federal government.[216] Thus, the practice of obtaining cybersecurity policy and adopting cybersecurity legislation should fall

[205] *Id.*
[206] Batchelder, *supra* note 130.
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *Id.*
[213] Lohrmann, *supra* note 192.
[214] *Id.*
[215] *Id.*
[216] Batchelder, *supra* note 130.

into the same critical state interest categories as elections, transportation, and intelligence.[217]

1. Preparation is Not Key

Many experts state that the most diligent approach to defeating ransomware is to prepare those who could be attacked.[218] Experts believe that the best approach to combat ransomware attacks is through preparation: ". . . following best practices such as regularly backing up data, educating employees about threats and risks and maintaining robust firewalls."[219] However, this approach has not worked since ransomware's creation in 1989; it is thirty years later and there has still been an increase in attacks since the original "AIDS Trojan" attack.[220] Attacks have continued to occur across the globe with hospitals, cities, and states unable or unwilling to upgrade all computer systems to "seal off vulnerabilities."[221] Preparation can help members know what to look for,[222] but the consequence stemming from robust prosecution is necessary to put a stop to the catastrophic malware attacks.

C. Measures to be Implements – Increase Funding for Cybercrime Prevention

CISA, the cybersecurity agency of the DHS, is dedicated to defending federal networks, election infrastructure, and physical security.[223] For Fiscal Year 2020, the House Appropriations Committee approved a $63.8 billion spending package for the DHS, with specifically two billion earmarked for CISA.[224] CISA's budget increased by $335 million from Fiscal Year 2019.[225] Representative Lucille Roybal Allard (D-CA) stated that the twenty-percent increase in funding will help CISA improve cyber and infrastructure defense systems faster.[226] Notably, CISA gained bipartisan support for increasing its

[217] *Id.*

[218] Neuhauser, *supra* note 13.

[219] *Id.*

[220] Waddell, *supra* note 7.

[221] Neuhauser, *supra* note 13.

[222] *Id.*

[223] Andrew Eversden, *The DHS Cyber Agency Gets Massive Funding Boost*, FIFTH DOMAIN (Dec. 17, 2019), https://www.fifthdomain.com/congress/capitol-hill/2019/12/17/the-dhs-cyber-agency-gets-massive-funding-boost/.

[224] Derek B. Johnson, *House Panel Approves $408 Million Boost for CISA*, FCW (June 11, 2019), https://fcw.com/articles/2019/06/11/dhs-approps-cisa-boost.aspx.

[225] *Id.*

[226] *Id.*

budget.[227] However, then-Director of CISA, Chris Krebs, requested $3.17 billion when testifying before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation for Fiscal Year 2020.[228] Krebs also requested $371 million for proactive cyber protection, providing CISA's National Cybersecurity and Communications Integration Center ("NCCIC") increased funding to quickly respond to incidents and risks.[229]

For Fiscal Year 2021, CISA has been approved for only $1.7 billion: "a significant budget cut from the more than two billion the agency received from Congress in December 2019."[230] While testifying before the House Homeland Security Committee, acting Secretary of the DHS, Chad Wolf, attempted to mitigate the congressional dismay regarding the funding decrease by hinting that it is possible for the CISA budget to be further decreased in 2021 since it is not an election year.[231] Although the CISA workforce grew by 500,[232] its budget dwindled by $258 million.[233] Representative Gary Peters (D-MI) claimed that state governments are not fiscally prepared to defend their constituents from attacks, stating: "State and local governments don't always have the tools to defend against cyberattacks. Financial constraints, workforce challenges, and outdated equipment are all serious challenges for states and cities."[234] Representative Cedric Richmond (D-LA) said a "cut of that magnitude" would harm American communities, and constituents would not be able to defend themselves against devastating cyberattacks.[235] As recognized by members of Congress, cuts to CISA's budget are detrimental to national security; all resources must be used to better handle emerging threats.[236]

1. COVID-19 Pandemic – The Need for More Funding

On December 31, 2019, scientists detected a new virus "in the city of Wuhan

[227] Kate Polit, *Bipartisan Support Emerges for Increasing CISA Funding*, MERITALK (May 1, 2019), https://www.meritalk.com/articles/bipartisan-support-emerges-for-increasing-cisa-funding/.

[228] *Id.*

[229] *Id.*

[230] Kate Polit, *DHS Acting Secretary Wolf Defends CISA Budget cut to Congress*, MERITALK (Mar. 3, 2020), https://www.meritalk.com/articles/dhs-acting-secretary-wolf-defends-cisa-budget-cut-to-congress/.

[231] *Id.*

[232] *Id.*

[233] Tim Starks, *Cyber Winners and Losers from Trump's Budget*, POLITICO (Feb. 11, 2020), https://www.politico.com/newsletters/morning-cybersecurity/2020/02/11/cyber-winners-and-losers-from-trumps-budget-785275.

[234] *Id.*

[235] Miller, *supra* note 14.

[236] *Id.*

in Hubei province, China"[237] and subsequently reported to the World Health Organization ("WHO").[238] On January 30, 2020, the outbreak was declared a "Public Health Emergency of International Concern."[239] Subsequently, on February 11, 2020, WHO announced that the name of the new disease is COVID-19.[240] COVID-19, also known as the coronavirus disease, has swept the entire globe, and has increased the overall demand for "medicine, vaccines, diagnostics, and reagents."[241] As a result of the growing pandemic, people have turned to the internet to stay updated, which has created a "perfect opportunity for hackers."[242] Malicious individuals have capitalized on the growing pandemic to "exploit and take advantage of the public and business[es]."[243]

An Android app called "COVID19 Tracker" portrayed itself as an app tracking the current outbreak. However, it was actually a form of ransomware locking owners out of their phones.[244] After the attacker locked the victim's phone, the attacker required that $100 in bitcoin be paid within forty-eight hours in exchange for the victim to regain control of the phone and its contents.[245] Cybersecurity researchers found multiple fake COVID-19 tracker maps that can infect computers, in addition to the apps that can infect phones.[246]

COVID-19 has created a stage for ransomware attackers to capitalize on growing fear sweeping the globe.[247] In the beginning of March, healthcare systems have been targeted by a new and dangerous Windows ransomware

[237] *Rolling Updates on Coronavirus Disease (COVID-19)*, WORLD HEALTH ORG., https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen (last updated Jul. 31, 2020).

[238] *Id.*

[239] *Id.*

[240] *Id.*

[241] *Medical Product Alert N°3/2020 Falsified Medical Products, Including In Vitro Diagnostics, that Claim to Prevent, Detect, Treat or Cure COVID-19,* WORLD HEALTH ORG. (Mar. 31, 2020), https://www.who.int/news/item/31-03-2020-medical-product-alert-n-3-2020.

[242] Antonio Villas-Boas, *A Fake Coronavirus Tracking App is Actually Ransomware that Threatens to Leak Social Media Accounts and Delete a Phone's Storage Unless a Victim Pays $100 in Bitcoin*, BUS. INSIDER (Mar. 16, 2020), https://www.businessinsider.com/coronavirus-fake-app-ransomware-malware-bitcoin-android-demands-ransom-domaintools-2020-3.

[243] Maggie Miller, *Top Agencies Warn Cybercriminals Are Using Coronavirus to Step up Hacking Efforts*, THE HILL (Apr. 8, 2020), https://thehill.com/policy/cybersecurity/491747-top-agencies-warn-cyber-criminals-are-using-coronavirus-to-step-up.

[244] Villas-Boas, *supra* note 242.

[245] *Id.*

[246] *Id.*

[247] Davey Winder, *Healthcare Workers Targeted by Dangerous New Windows Ransomware Campaign Using Coronavirus as Bait*, FORBES (Mar. 22, 2020), https://www.forbes.com/sites/daveywinder/2020/03/22/healthcare-workers-targeted-by-dangerous-new-windows-ransomware-campaign-using-coronavirus-as-bait/#320f0b382212.

threat.[248] The threat is called “NetWalker,” and it is used by cybercrime groups that have created phishing attacks against the healthcare sector during the early stages of COVID-19.[249] NetWalker lures its targets in with an email about COVID-19,[250] then attacks by locking down the computer or specific websites.[251] The Champaign Urbana Public Health District (“CHUPD”) in Illinois, which covers 210,000 citizens and the University of Illinois, was attacked by NetWalker in early March 2020.[252] The malware attacked CHUPD’s primary website, and forced the district to set up an alternate website to keep citizens updated about the growing COVID-19 pandemic.[253]

Additionally, ransomware attackers have targeted systems abroad, such as Hammersmith Medicines Research, a London-based company that conducts medicinal clinical trials.[254] While the company was in talks about testing a potential COVID-19 vaccine, hackers locked thousands of patient records and threatened to publish the information if a ransom was not paid.[255] André Pienaar, founder of venture capital firm C5 Capital, stated that cybersecurity companies have seen “a number of instances where clinical labs involved in testing, or major hospitals, have suffered ransomware attacks, where all their IT systems have been knocked down.”[256] Ransomware attackers have been attempting to seek profits from the global crisis, and the ramifications could be devastating.[257]

Malcolm Taylor, head of cybersecurity at ITC Secure, said, “the attackers know that these organizations are so desperate at the moment to build ventilators, or to stop people from getting sick, and they are trying to exploit that.”[258] Furthermore, organizations have turned to a remote workforce, creating an opportunity for ransomware attackers to target gateway and virtual private network appliances.[259] Now more than ever, cybersecurity officials have recommended that hospitals regularly update their technology services, strengthen protocols in response to breaches, and engage with security

[248] *Id.*

[249] *Id.*

[250] *Id.*

[251] Shaun Nichols, *Fresh Virus Misery for Illinois*, THE REGISTER (Mar. 12, 2020), https://www.theregister.co.uk/2020/03/12/ransomware_illinois_health/.

[252] *Id.*

[253] *Id.*

[254] Ryan Gallagher & Bloomberg, *Hackers ‘Without Conscience’ Demand Ransom from Dozens of Hospitals and Labs Working on Coronavirus*, FORTUNE (Apr. 1, 2020), https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/.

[255] *Id.*

[256] *Id.*

[257] *Id.*

[258] *Id.*

[259] Samuel Haig, *Microsoft Helps Hospitals Fight Ransomware Amid Coronavirus Pandemic*, COINTELEGRAPH (Apr. 7, 2020), https://cointelegraph.com/news/microsoft-helps-hospitals-fight-ransomware-amid-coronavirus-pandemic.

professionals on a more regular basis.[260]

In response to the growing cyberthreat, CISA issued an alert that organizations keep all technology systems up to date and remain transparent with employees about the dangers of ransomware.[261] Since January 2020, more than 4,000 coronavirus-themed web domains have emerged. Cyber group Check Point estimates that "5 percent [of the web domains] were suspicious and 3 percent were malicious."[262] The repeated message from CISA to all organizations is to ensure all employees are educated about the potential threats that may appear as a result of the pandemic.[263] Cyber experts have stated that although USTelecom has pledged to protect against network vulnerabilities, it is imperative that Congress provides greater funding to CISA and to the cybersecurity of critical infrastructure.[264]

IX. CONCLUSION

There is more that can be done in response to ransomware in the US. A response to the growing threat must be through jurisprudential, political, and financial means. The number of ever-increasing attacks can be impeded through criminal deterrence,[265] US cybercriminal tribunals,[266] a local government focus on cybercrime,[267] and an increase in federal funding for CISA.[268] To keep the US and its citizens safe, the federal government, in conjunction with state legislatures, must put its full force behind cybersecurity management.

[260] *Id.*

[261] Maggie Miller, *Hackers Find New Target as Americans Work from Home During Outbreak*, THE HILL (Mar. 14, 2020), https://thehill.com/policy/cybersecurity/487542-hackers-find-new-target-as-americans-work-from-home-during-outbreak.

[262] *Id.*

[263] *Id.*

[264] *Id.*

[265] *See* Drumbl, *supra* note 11, at 264 (discussing the development of legal responses for international crime); *see also* Ladegaard, *supra* note 11, at 2 (discussing whether crime rates drop after highly publicized trials); *see also* Staal, *supra* note 11, at 428 (describing the principle of extraterritorial criminal jurisdiction).

[266] U.S. CONST. art. I, § 8, cl. 9; Perloff-Giles, *supra* note 12, at 226.

[267] Neuhauser, *supra* note 13; *see also* Uwizeyemungu & Poba-Nzaou, *supra* note 5.

[268] Miller, *supra* note 14.