Ransomware: The Blame Stops Here

by

Marissa Wolfson

Table of Contents

Abstract ----------i

Introduction ----------1

Ransomware Attackers----------1

Operating System Providers----------4

Government Agencies ----------6

IT Professionals----------8

Cyber-Security Companies----------10

A. Contract Fulfilment Post-Attack----------12

Third-party Vendors----------13

Low-Level Employees----------15

City Officials and Other "People in Charge"----------17

Policy Implications----------21

Conclusion----------22

Abstract

Ransomware is a growing problem. In 2019, it plagued nearly 1000 U.S. businesses, institutions, and municipalities. The nature of these attacks makes it nearly impossible to hold perpetrators accountable, leaving some victims without a feeling of justice or the financial funds to recover. In response, some victims are beginning to shift liability away from attackers and towards IT specialists, cybersecurity companies, and developers of vulnerable computer operating systems. Additionally, some experts believe liability could extend much further in the future, potentially implicating government officials, company board members, third-party vendors, and even the employees whose specific devices are infected with malware. Though it may seem like the only way to seek justice (and potentially monetary relief) following a ransomware attack, assigning legal liability to these actors advances a victim-blaming mentality that shifts the focus away from the actual attackers. While some actors may very well have acted negligently and can be held accountable, there is a fine line between true negligence and using an actor as a scapegoat. As such, ransomware victims should think very carefully before assigning legal liability to an actor other than the attacker.

Introduction

In 2019, at least 966 healthcare providers, municipalities, and education providers were hit with ransomware attacks, costing victims in excess of $7.5 billion.[1] Devastatingly, the sophisticated hackers behind these attacks are almost never caught, leaving many victims not only in a financial bind, but lacking a sense of justice.[2] Without so much as a face nor a name to link to the crimes, the question remains: who should face the blame after a ransomware attack? Unsurprisingly, this question is being answered in a variety of ways. As detailed in the sections below, some victims have started looking at IT professionals and cybersecurity companies who they believe should have exercised more diligence to prevent the attack. Other victims focus on governmental or company officials with the purse strings who chose not to fund the technology necessary to protect a computer system from attack. Even still, other victims attempt to blame software companies like Microsoft or the federal government itself when attacked.

As illustrated in these scenarios, there is a tangled, messy web of actors who may be accused of negligence after a ransomware attack. Litigation or (potentially wrongful) termination of an employee may seem the only way to regain lost funds or deter future negligence. However, a closer look into many of the actors who could be liable post-ransomware attack reveals that trying to assign blame may be a misguided and complicated task.

Ransomware Attackers

There is little question as to whether those who initiate ransomware attacks should be held liable for their illegal actions. However, obtaining such justice is nearly impossible due to the methods attackers use to remain anonymous. Ransomware attackers, who fall under the

[1] *The State of Ransomware in the US: Report and Statistics 2019*, EMISOFT MALWARE LAB, https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/ (last visited May 15, 2020).
[2] *Id.*

general umbrella of cybercriminals, typically use secure proxy servers to maintain anonymity, which hide their location and route their communications through multiple countries to avoid detection.[3] Cybercriminals also protect themselves from getting caught by committing cybercrimes in countries where they will not be prosecuted for their actions.[4] Consequently, catching ransomware attackers is no easy task.

Efforts to catch cybercriminals typically involve coordination between law enforcement, government agencies, international partners, and private corporations.[5] These coordinated efforts, sometimes dubbed "task forces", [6] spend thousands of hours performing cyber forensic analysis and research in order to create data that may be used as evidence in court.[7] Task forces also spend countless hours decrypting files, cracking passwords, and recovering lost data after a ransomware attack.[8] Sadly, these time-consuming and resource-draining efforts have had but marginal success in identifying ransomware attackers.

Another huge challenge in catching ransomware attackers is being able to prosecute attackers for their crimes in the United States.[9] As mentioned previously, ransomware attackers often choose to initiate attacks in countries, such as those Eastern Europe, that do not have active extradition treaties with the United States.[10] It is also difficult to convince foreign governments to prosecute the attackers in their own courts of law.[11]

---

[3] *How Do Cybercriminals Get Caught*, NORTON.COM, https://us.norton.com/internetsecurity-emerging-threats-how-do-cybercriminals-get-caught.html (last visited March 27, 2020).
[4] *Id*.
[5] *Id*.
[6] Task forces are generally created to complete the most technically complicated tasks, and often are supported by the FBI and NW3C (National White Collar Crime Center). *See id*. at 3.
[7] *Id*.
[8] *Id*.
[9] John Abel et al., *Ransomware: The Cutting-Edge Cybercrime Taking Over the Country and What You Can Do to Stop It*, 1 Nat'l. Ass'n of Attorney Gen. 4 (2016).
[10] *Id.*
[11] *Id.*

Although it is difficult to identify ransomware attackers, it is not impossible. In 2018, a federal grand jury indicted two Iranian men, Shahi Savandi and Mohammad Mehdi Shah, of international computer hacking and extortion.[12] According to the indictment, Savandi and Shah created the Ransomware known as *SamSam*, which would enter victims' computers through security vulnerabilities and would encrypt the victims' data.[13] Over 200 businesses and municipalities fell victim to *SamSam* ransomware, the most notable being the City of Atlanta.[14] Through *SamSam* ransomware, Savandi and Shah allegedly cost their victims more than $30 million in losses.[15] Despite the District of New Jersey issuing a federal arrest warrant for the men, Savandi and Shah are still at large and secured a position on the FBI's most wanted list for cybercriminals.[16]

Holding ransomware attackers liable for their actions becomes even more difficult when attackers have support or protection from their country's government. On September 6, 2018, the US Department of Justice charged Park Jin Hyok, a computer programmer from North Korea, with creating *WannaCry* ransomware.[17] *WannaCry*, an infamous form of malware that was behind some of the biggest cyber-attacks in recent history, targeted computers using Microsoft Windows and encrypted the data of unsuspecting victims.[18] The DOJ discovered Park was an

---

[12] *Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses*, DEPARTMENT OF JUSTICE OFFICE OF PUBLIC AFFAIRS, https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public (last visited May 16, 2020).
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] Savandi and Shah secured a place on the 2018 FBI Most Wanted list for Cybercriminals under the general name of "SamSam Subjects." *See FBI Most Wanted: Samsam Subjects*, FBI.GOV, https://www.fbi.gov/wanted/cyber/samsam-subjects (last visited May 16, 2020).
[17] Catalin Cimpanu, *How US authorities tracked down the North Korean hacker behind WannaCry*, ZDNET.COM, (Sep. 6, 2018), https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/.
[18] *Id.*

active member of the Lazarus Group, a government-sponsored hacking group.[19] Though no North Korean government officials were specifically named by the DOJ, their indicting document implicated the North Korean government generally, saying the government managed the phony company Hyok allegedly was an "online game developer" for.[20] As of April 2020, Hyok has evaded the DOJ's charges and secured a spot on the FBI's most wanted list.

Whether the North Korean government was in fact behind the *WannaCry* attacks that Hyok was charged with, the inability to extradite him from North Korea shows attackers have yet another layer of protection against accountability for their actions. In 2020, there were 67 countries that did not have extradition treaties with the United States.[21] Ransomware attackers are quite aware of this.[22] There is also a handful of countries, such as Ecuador, Cuba, Iceland, Switzerland, and Venezuela, who have extradition treaties with the United States but still refuse extradition requests.[23]

While there is little controversy regarding whether ransomware attackers should face responsibility for their actions above all other actors, the low chances of catching the attackers and the high probability they will evade punishment even if identified invites the question: who else is liable?

Operating System Providers

As the number of ransomware attacks increases, more patterns are prevalent from collected data. One such pattern, as explained by the Cybersecurity and Infrastructure Security Agency (CISA), is that most attackers target victims using outdated applications and operating

[19] *Id.*
[20] *Id.*
[21] *Countries Without Extradition 2020*, WORLD POPULATION REVIEW, https://worldpopulationreview.com/countries/countries-without-extradition (last visited April 19, 2020).
[22] *See supra*, note 9.
[23] *Id.*

systems.[24] Out-of-date applications and operating systems often are not equipped with security measures that keep users safe against ransomware attacks, which leads some to wonder if companies that provide operating systems that are vulnerable to attacks should be held liable.

This issue came to life in 2014 when Microsoft announced it would stop supporting Windows XP, and returned when Microsoft announced in 2020 that it would no longer support Windows 7.[25] The decisions to stop supporting these systems were made with full knowledge that many businesses and municipalities still use them. Microsoft surprised many by releasing security updates for versions of Windows it no longer supports,[26] in an attempt to protect devices from *WannaCry* malware. A move like this can be interpreted in multiple ways. First, it shows that Microsoft cares about its customers who are still using old products, by providing them with a way to stay protected from the growing threat of ransomware. Alternatively, it can be read as Microsoft understanding the responsibility it has when its customers are susceptible to ransomware through flaws in its operating systems.

This practice is criticized for putting users at risk for ransomware vulnerability. Software updates for programs such as Windows XP are not obtainable unless customers running this operating system pay for "customer support." According to Zeynep Tufecki, associate professor at the School of Information and Library Science at the University of North Carolina, "Companies like Microsoft should discard the idea that it can abandon people using older software." Tufecki added, "The money they made from these customers hasn't expired; neither has their responsibility to fix defects."[27]

---

[24] *Ransomware*, CISA, https://www.us-cert.gov/Ransomware (last visited Apr. 19, 2020).
[25] Nicholas De Leon, *Microsoft Has Ended Support for Windows 7. Now What?*, CONSUMERREPORTS.ORG, (Jan. 14, 2020), https://www.consumerreports.org/computers/microsoft-ends-windows-7-support/.
[26] Nick Wingfield, *In Ransomware Attack, Where Does Microsoft's Responsibility Lie?*, THE NEW YORK TIMES, (May 15, 2017), https://www.nytimes.com/2017/05/15/technology/cyberattack-microsoft-software-responsibility.html.
[27] *Wingfield*, *supra* note 26, at 2.

A prime example is Microsoft's decision to stop providing free support for Windows 7 users in January 2020. This decision is particularly concerning when one considers that 31 percent of federal civilian agency computers still ran on Windows 7, as of June 2019.[28] As of May 2019, more than 25 percent of medical devices were running on Windows 7, and 16.6 percent of U.S. healthcare IT professionals did not have the ability to patch operating systems.[29] This begs the question of why funding is not being allocated to updating systems, which may shift liability into the hands of city officials and company board members.

In addition, most software companies require customers to sign End User License Agreements, in which customers essentially agree to being responsible for maintaining their own systems and to not blame the software company if anything goes awry.[30] Customers who sign these contracts make it infinitely more difficult to sue the software company in the wake of a ransomware attack, as they would likely have to prove the contract is unenforceable before being able to successfully go this route. Still, it may be worth pursuing if a situation arose where a software company was glaringly negligent in producing and patching software that was later exploited.

Government Agencies

When experiencing backlash for abandoning old systems, Microsoft has largely stayed silent. However, the company did speak up when accused of facilitating ransomware through such abandonment. In its response, Microsoft attempted to shift the blame to the National Security Agency (NSA), claiming it was the NSA that developed the malware that exploited a

[28] Andrew Eversden, *Are federal agencies prepared for the end of free Windows 7 support?*, FEDERAL TIMES, (Aug. 14, 2019), https://www.federaltimes.com/it-networks/2019/08/14/are-federal-agencies-prepared-for-the-end-of-free-windows-7-support/.
[29] Fred Donovan, *One-Quarter of Medical Devices Still Running Outdated Windows 7*, HITINFRASTRUCTURE, (May 7, 2019), https://hitinfrastructure.com/news/one-quarter-of-medical-devices-still-running-outdated-windows-7.
[l]https://securitycurrent.com/massive-ransomware-attack-can-i-sue/.

Windows vulnerability, and fell into the wrong hands.[31] Such an accusation came from Microsoft's chief legal officer, Brad Smith, who tried to shift blame to users who do not update their operating systems in addition to intelligence agencies who practiced "the stockpiling of vulnerabilities."[32] Smith's latter comment refers to the NSA's creation of *Eternal Blue*, a cyberattack exploit.[33] *Eternal Blue* was ultimately poached from the NSA by hackers called "Shadow Brokers."[34] Ironically, the NSA created *Eternal Blue* as a technique to exploit software flaws for intelligence purposes.[35]

In the United States, the Federal Torts Claim Act allows the federal government to be sued for torts, such as negligence, just as private individuals can be.[36] Therefore, the question arises whether the NSA could be sued for negligently failing to secure its cyberweapons. However, there would likely be significant hurdles in such litigation.

A historical example may provide insight. In the aftermath of World War II, the Department of Defense was sued for negligently failing to secure its weapons, which caused damage to a nearby neighborhood and its residents.[37] However, lawsuits against the Department of the Defense were largely unsuccessful because there is no governmental liability for the

---

[31] AOMI, *Who Should be Responsible for Ransomware Attack*, UBACKUP.COM, (Oct. 9, 2019), https://www.ubackup.com/anti-ransomware/who-should-be-responsible-for-ransomware-attack-1234.html.
[32] Mark Fritz, *The Blame Game: The Definitive Guide to Who's at Fault for The Ransomware Cyberattack*, BENZINGA, (May 22, 2017), https://www.benzinga.com/news/17/05/9496220/the-blame-game-the-definitive-guide-to-whos-at-fault-for-the-ransomware-cyberatta. (Smith wrote "We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world…An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen.")
[33] *AOMI*, *supra* note 31, at 6.
[34] The identities of the shadow brokers are unknown. However, some suspects include former intelligence community contractors or Russian hackers. *Who are the Shadow Brokers?*, CYBERSECURITYINTELLIGENCE.COM, https://www.cybersecurityintelligence.com/blog/who-are-the-shadow-brokers-2684.html (last visited May 16, 2020).
[35] *Fritz*, at 2.
[36] *Rasch*, at 3.
[37] *Id*.

negligent exercise of uniquely governmental functions.[38] A similar outcome would be likely in litigation against the NSA, as the creation of cyber-security exploits is likely to be classified as a uniquely governmental function.

For argument's sake, if a court determined the NSA could be found negligently liable for their actions, plaintiffs would have to prove that (1) the NSA had a duty to prevent hacks from ransomware attackers (2) the breach was well-known to all; and (3) there was no "efficient intervening cause" causing the damages.[39] Each factor is arguably debatable in this context. The most compelling argument stems from the first requirement: the NSA may have a general duty to protect its classified information and cyberweapons from attackers. However, proving this universally understood concept may be difficult, especially in a court system that is still adapting to the modern era of ever-expanding technologies. The counterargument to this would be the NSA cannot be responsible for its property falling into the wrong hands through individual employees or users. In the same way that the Social Security Administration is not liable for theft of an individual's social security card, the NSA should not be liable for having their property stolen from them, even if that property has the potential to cause damage in the wrong hands.

IT Professionals

Another actor who sometimes faces blame in the wake of a ransomware attack is the IT professional responsible for the victim's cybersecurity measures. The theory behind finding an IT professional negligent after a ransomware attacking is fairly straightforward: if the employee had been doing his or her job correctly—keeping the highest of security measures in place and maintaining a watchful eye on network intrusions—the ransomware attack would not have

[38] *Dalehite v. United States*, 346 U.S. 15 (1953) (holding the FTCA restricts a waiver of liability only to situations in which a private citizen would also be liable).
[39] *Id.*

occurred. In reality, the IT professionals' abilities to successfully do their jobs often hinges on the budget they receive. A recent study by the *National Association of State Chief Information Officers* found that, on average, less than 3 percent of state IT budgets are dedicated to cybersecurity.[40] Such a statistic drives home the reality that IT professionals can only do so much with what they have. If a company or municipality has not provided enough room in its budget to purchase new hardware, up-to-date operating systems, and off-site backup systems, IT employees are not equipped with the proper tools to keep their systems safe from ransomware. Still, IT professionals are some of the easiest actors to accuse when something technologically awry, such as ransomware, occurs.

Nevertheless, the decision to shift the blame away from the attacker and onto an IT professional is not without controversy. Such was the case in Lake City, Florida, which was attacked and had its data held for ransom in July 2019. In the aftermath of the attack, Lake City officials fired the IT specialist who was responsible for keeping the city's computer system protected from cyber threats. The specialist, Brian Hawkins, fired back against Lake City, suing the city for ruining his reputation in the media, using him as a scapegoat, and firing him on improper grounds.[41]

In his suit, Hawkins claimed that he recommend two years prior that Lake City increase the budget for cybersecurity measures. Specifically, he "warned the city about its vulnerability long ago—urging the purchase of an expensive, cloud-based backup system that might have averted the need to pay a ransom."[42]

---

[40] Samantha Ann Schwartz, *The forgotten ones: Ransomware preys on the resource-poor*, CIO DIVE, (Oct. 17, 2019), https://www.ciodive.com/news/the-forgotten-ones-ransomware-preys-on-the-resource-poor/565062/.
[41] Greg Edwards, *Ransomware Fall-Out of Lake City, Florida*, CRYPTOSTOPPER, (Sep. 3, 2019), /ransomware-fall-out-of-lake-city-florida.
[42] Frances Robles, *When Ransomware Cripples a City, Who's to Blame? This I.T. Chief Is Fighting Back*, THE NEW YORK TIMES, (Aug. 22, 2019), https://www.nytimes.com/2019/08/22/us/florida-ransomware-hacking-it.html.

Hawkins was not the only I.T. employee who lost his jobs after a ransomware attack. Two high-level I.T. employees, including one who had served as an acting director, were fired after a ransomware attack crippled the city of Baltimore's system in 2019.[43] A spokesperson for the mayor of Baltimore went on record stating that no one in the city's government was to blame for the attack, and blame should be assessed to the attackers.[44] However, Baltimore officials would not comment as to why I.T. employees were fired, claiming the dismissals were confidential personnel issues.

Chief Information Officer Frank Johnson was one of Baltimore's former employees who was terminated shortly after the ransomware attack.[45] Johnson's response to the ransomware attack was sharply criticized, as he was faulted with not communicating properly with agencies impacted by the ransomware attack, and he was blamed for how expensive cleanup measures were.[46] This shifts the question away from whether an I.T. employee can be fired for preparing a company for an attack to whether an I.T. employee can be fired for improperly responding to the attack. These examples highlight the desire of some companies to hold someone accountable after a ransomware attack.

Cyber-Security Companies

As ransomware becomes an increasingly worrisome threat for companies and municipalities, cyber-security companies find themselves on the front line of defense against attackers. Such companies are tasked with fighting cyberthreats—including ransomware attacks.

---

[43] Ian Duncan, *Two senior managers at Baltimore's IT department replaced during recovery from ransomware attack*, THE BALTIMORE SUN (Aug. 9, 2019), https://www.baltimoresun.com/politics/bs-md-ci-it-staffing-20190809-egcxxq7n7jawjcrbopjglnat3y-story.html.
[44] *Id.*
[45] Benjamin Freed, *Baltimore CIO, scrutinized for ransomware response, no longer with city*, STATE SCOOP, (Oct. 7, 2019), https://statescoop.com/baltimore-cio-frank-johnson-no-longer-with-city-ransomware/.
[46] *Id.*

Should a company that claims to protect computer systems from viruses like ransomware be held liable if the systems are attacked?

Alternatively, what if a cyber-security company fails to even detect the ransomware? This was the question posed in a class-action lawsuit against Electronic Health Record vendor Allscripts. Allscripts was hit with a ransomware attack in January 2018, which encrypted the health records of many consumers.[47] Plaintiffs in the suit were Allscripts customers who were negatively affected by Electronic Health Record downtime post-attack.[48] While some plaintiffs were able to access client records within hours after the attack, some were not able to access records for a week.[49] As a result, plaintiffs requested damages for lost revenue and disruption of business.

Allscripts Healthcare Solutions LLC, whose parent company is Allscripts Healthcare Solutions Inc., was responsible for implementing its own cybersecurity and privacy measures.[50] Plaintiffs alleged that Allscripts failed to secure and audit its system, ultimately leading to the attack.[51] Even more alarming, plaintiffs alleged Allscripts was aware of "deficiencies in its products and services [that] could result in privacy and security vulnerability or compromises and failed to take adequate measures to protect against any such event."[52]

The case was ultimately thrown out on a technicality; a federal judge ruled the suit was directed towards improper entity Allscripts Healthcare Solutions Inc., instead of Allscripts Healthcare Solutions LLC. Such a result leaves largely unanswered the question of whether a

[47] Jackie Drees, *Cybersecurity lawsuit against Allscripts tossed by judge*, BECKER'S HOSPITAL REVIEW, (June 6, 2019), https://www.beckershospitalreview.com/ehrs/cybersecurity-lawsuit-against-allscripts-tossed-by-judge.html.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] Jessica Davis, *Allscripts sued over ransomware attack, accused of 'wanton' disregard*, HEALTHCARE IT NEWS, (Jan. 26, 2018), https://www.healthcareitnews.com/news/allscripts-sued-over-ransomware-attack-accused-wanton-disregard.
[52] *Id.* at 2.

cyber-insurance company may be held liable for failing to detect ransomware. Still, the suit turned heads in world of cyber-security, as customers and security firms alike started taking a closer look at just how protective a security system truly is against invasive ransomware attacks.

A. Contract Fulfilment Post-Attack

This concern over the reliability and efficiency of cyber-security measures in handling ransomware attacks was given a name—and case number—in May 2018. Industrial Fabricators, Inc. filed suit against its cybersecurity provider, Alt-Net Services - Charlotte, Inc. for cybersecurity negligence.[53] Industrial Fabricators claimed Alt-Net was negligent in maintaining appropriate security, leaving them susceptible to a ransomware attack.[54] This was one of many reasons that Industrial Fabricators terminated its relationship with the provider, despite allegedly failing to pay nearly $50,000 in services rendered. The court ultimately denied Alt-Net's arguments for lack of standing and the doctrine of estoppel.[55] However, the court did not provide a clear stance on whether it is permissible to terminate a contract without paying for services rendered when hit with ransomware.

Despite the door being left open for future lawsuits regarding this issue, contract law makes it clear that cyber-security companies can have safeguards in place to protect themselves from a client's breach in the wake of an attack. First and most simply, a company can have a provision in their contract to reiterate a client's duty to continue adhering to a contract, despite being attacked. Such a provision would also likely address the cybersecurity company's liability, if any, in the wake of an attack. This option hinges on society's willingness to see a ransomware

[53] *Industrial Fabricators, Inc. v. Alt-Net Services—Charlotte, Inc.*, No. 17 CVS 84, 2018 WL 2148613 (Super. Ct. N.C. May 9, 2018).
[54] *Id.*
[55] *Id.*

attack as a foreseeable issue needs to be covered in a contract.[56] With an ever-increasing amount of ransomware attacks across the globe, attacks against companies and municipalities with sensitive data does not seem as unforeseeable as once thought.

Another way to prevent a lawsuit regarding a breach of a contract is by classifying a ransomware attack as an event that would trigger a force majeure clause.[57] Force majeure clauses relieve one or both parties of their contractual obligations if an event specified in the clause occurs.[58] While typical examples of such events include natural disasters, epidemics, and wars, parties may consider adding ransomware attacks to the list. This classification is fitting when one considers the true nature of a ransomware attack as being a third-party intrusion on the contract that may leave some parts of it unfulfillable.

Third-Party Vendors

Many companies choose to outsource their IT services to third parties in order to increase efficiency. However, the decision to use third party vendors can be risky; third-party software controlled or provided by outside vendors can be difficult to patch, which leaves computers vulnerable to ransomware attacks.[59]

In 2016, half of all healthcare organizations participating in a *Ponemon* survey[60] reported they had experienced a data breach caused by a third-party vendor's exploitative software.[61] Particularly in the healthcare space, a data breach means personal information, such as medical

---

[56] Cripps Pemberton Greenish, *Ransomware: using contractual terms to protect yourself from the consequences*, CRIPPSPG, (June 9, 2017), https://www.crippspg.co.uk/ransomware-using-contractual-terms-protect-consequences/.
[57] *Id.*
[58] *Id.*
[59] Tony Howlett, *Top 3 threats posed by third-party vendors*, SECURE LINK, (Oct. 9, 2019), https://www.securelink.com/blog/top-3-threats-posed-by-third-party-vendors/.
[60] Ponemon Institute conducts research on consumer trust, privacy, data protection and emerging data securities technologies and conducts surveys to obtain such information. *Ponemon Institute Research*, About Us, https://www.ponemon.org/about-ponemon-research (last visited March 19, 2020).
[61] Other well-known companies who were attacked because of vulnerabilities in third-party software include Equifax, Tesla, Universal Movie Group, and more. *Supra*, note 45, at 2.

records, is confiscated. Consequently, companies should be very wary of which third-party vendors they trust and how much access the vendors have to client information.

One way to limit the vulnerability created by using a third party is to limit the party's access to systems and data. By giving the third party only the information needed to perform its duties, client records and other critical data can stay close to the company. As a result, ransomware attackers who access systems through exploiting the third-party vendor may be less capable of accessing vital information that would, if encrypted, entice a company to pay a ransom.

Still, companies should be wary of using third parties for IT work or cybersecurity because companies have been found liable for the negligent actions taken by their vendors. Though it may not be initially apparent, ransomware is a form of data breach that results in a loss of control in data for a company.[62] Therefore, the liability generally assessed for negligence in a traditional data breach case could apply to a company who negligently allowed a ransomware attack to occur. In a traditional data breach case, liability is imposed if the entity failed to do the following: (1) implement safeguards required by statute or reasonable security measures; (2) remedy or mitigate the damage once the breach occurred; or (3) timely notify the affected individuals under a state's data breach notification statute, which could give rise to liability for civil penalties imposed by a state attorney general or other state enforcement agency.[63] While these factors generally apply when an individual (or group of individuals in a class-action) are

[62] According to the Department of Health and Human Services, ransomware attacks are considered security incidents, which are attempted r successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *Fact Sheet: Ransomware and HIPPA*, DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://www.hhs.gov/sites/default/files/RansomwareFactSheet (last visited Apr. 30, 2020).

[63] *Who is liable when a data breach occurs?*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability (last visited Apr. 30, 2020).

alleging negligence, it is important to consider that a company who uses a third-party vendor who is guilty of one or more of these factors may also be negligent.

Using third-party vendors is a cost-efficient and common way for companies to satisfy their IT and cybersecurity needs but doing so can open a company up to extra risk. As a general point, when using a third-party vendor to complete a task, a company is giving away their ability to fully control that task. When the task is something as critical as keeping a computer system running and protected, the risk may outweigh the benefit. If a vendor is the most viable option for a company, the vendor should only receive access to what they need to satisfy their duties. And perhaps most crucially, if a company uses a third party and has data encrypted or lost through a ransomware attack, they should accept they may be found negligent as well.

Low-Level Employees

Most ransomware attacks occur through methods aimed at deceiving employees who inadvertently grant them access to the network.[64] Many victims do not have advanced technical knowledge needed to avoid falling victim. Ransomware most frequently spreads through virus-ridden files or links distributed in phishing emails.[65] The emails often deceive employees by appearing to be from coworkers, supervisors, or well-known companies, such as Microsoft. When an employee clicks on the link or tries to open the file, the computer is infected with the ransomware.[66] Files within the computer system become encrypted and inaccessible.

---

[64] Ransomware: Common Attack Methods, PALO ALTO NETWORKS CYBERPEDIA, https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods (last visited May 22, 2020).
[65] *Jason E. Thomas*, Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks, 13, INT'L JOURNAL OF BUSINESS AND MANAGEMENT, 1, 1 (2018).
[66] Such a tactic is commonly referred to as spear-phishing, which is "an email or electronic communications scam targeted towards a specific individual, organization or business," which appears to be from a trustworthy source. Spear-phishing uses social engineering techniques to trick employees and top executives alike. *See What is Spear Phishing? – Definition*, KASPERSKY.COM, https://usa.kaspersky.com/resource-center/definitions/spear-phishing (last visited May 22, 2020).

Ransomware can also spread through "exploit kits" which are toolkits that are planted on websites frequented by employees.[67] The exploit kits probe visitors' devices for exploitable vulnerabilities and then download and run ransomware on an individual's device. Companies are at risk of losing all their data due to the actions of just one employee, who could be anyone from the lowest-level worker to the CEO.

In theory, ransomware is less successful at infecting systems if an employee is adhering to the guidance given by IT professionals and cybersecurity specialists. Most individuals who have worked in an office have received emails from IT telling them to stay up to date on their security patches and to install the latest operating system updates when they are available. If an employee chooses to ignore these warnings, typically the fallout is nothing more than a mere reprimand or an automatic update at an inconvenient time. However, if an employee ignores these warnings and then falls victim to a ransomware attack, it poses the question of whether their negligence could make them liable, in part, for the attack.

When assigning liability to a low-level employee, an issue of deep-pockets versus shallow-pockets arises. Low-level employees are likely unable to pay the kind of money needed to recover from ransomware. If a company were to file suit against their own employee to recover funds lost in ransomware cleanup, the cost of litigation alone would likely outweigh what could be gained from the employee.

Even if a company were to decide to pursue a lawsuit against an employee for his or her negligence leading up to a ransomware attack, it may be difficult to prove the employee was, in fact, negligent. If an employee had very limited technical skills and was unaware of his or her negligent behavior, proving the employee had the understanding that their behavior was

[67] *Crypto-ransomware*, F-SECURE.COM, https://www.f-secure.com/en/web/labs_global/crypto-ransomware (last visited May 22, 2020).

negligent would be extremely difficult. While this may not be the case in some instances when employees ignore critical update notifications and straightforward communications requesting them to comply with the updates, each situation would likely need to be analyzed on a case-by-case basis.

Another wrinkle in the ability to prove a low-level employee's negligence is the effectiveness of the training. Now more than ever before, companies and municipalities should be implementing cyber-safety awareness trainings to inform employees on the issue of ransomware and teach them how to stay protected. However, these trainings do not have perfect track records against ransomware. While they can help reduce the chance of employees falling for a phishing email or related scam, they cannot eliminate the risk entirely.

A question that arises from increased employee training is at what point—if any—does falling for a scam that an employee should be aware of become negligent behavior? For example, if an employee is trained not to click on suspicious links, and then two months later clicks on a suspicious link and their computer is infected with ransomware, would they be more negligent than if they had not received the training? The simple answer is yes, but the effectiveness of the training, whether there was a certification course involved, and how long it had been since the training can influence the liability determination. Consequently, finding employees liable for negligence in a ransomware attack would be a waste of time and resources.

City Officials and Other "People in Charge"

When a company or municipality has been hit with ransomware, whoever is bestowed with decision-making power faces a very difficult question: should they pay the ransom? One may wonder why any entity would pay a ransom, which ultimately gives the attacker exactly

what they want. In theory, if victims stopped paying ransoms, there would be no incentive for attackers to continue, and this would lead to the end of ransomware altogether.

In actuality, the decision whether to pay a ransom or not is far more complex. In many cases, paying a ransom is the most financially-sound decision. Between the last quarter of 2019 and the first quarter of 2020, the average ransom demanded by attackers was about $111,000.[68] This amount, while substantial to smaller companies and municipalities, is but a fraction of the cost that could come from rebuilding entire systems and recovering encrypted data—the sad fate an entity who chooses not to pay a ransom will surely face.

The number of victims who choose to pay the ransom has grown from 39 percent in 2018 to nearly 58 percent in 2020.[69] The significant growth may be attributable to the fact 67 percent of ransom payers reported recovering their data after paying the ransom.[70] For those victims, the ransom was likely a small price to pay to avoid hefty recovery costs.

The City of Baltimore was put in this very situation in May 2019, when attackers encrypted data on nearly 10,000 government computers.[71] Attackers demanded $76,000 in bitcoin, which city officials refused to pay.[72] Their decision would ultimately cost the city close to $10 million in cleanup costs.[73] While there was no guarantee that paying the ransom would have ensured the decryption of their files, thus rendering the exorbitant cleanup costs nonexistent, the city officials were heavily critiqued for their choice not to pay.

---

[68] Filip Truta, *Successful Ransomware Infections Surge to Record in 2020 as Victims Grow More Willing to Pay, Research Shows*, SECURITY BOULEVARD, (Apr. 3, 2020), https://securityboulevard.com/2020/04/successful-ransomware-infections-surge-to-record-in-2020-as-victims-grow-more-willing-to-pay-research-shows/.
[69] *Id.*
[70] *Id.*
[71] Bruce Sussman, *Baltimore, $18 Million Later: 'This Is Why We Didn't Pay the Ransom'*, SECUREWORLD.COM (Jun. 12, 2019), https://www.secureworldexpo.com/industry-news/baltimore-ransomware-attack-2019.
[72] *Id.*
[73] *Id.*

Still, Baltimore city officials stood by their decision not to pay the ransom and fuel future ransomware attacks. Baltimore is not the only city whose leaders have elected not to pay a ransom. In 2018, the City of Atlanta was hit with a cyberattack. Hackers demanded $51,000 worth of bitcoin, but Atlanta officials announced that they did not pay the ransom—a decision that would cost the city $2.6 million dollars in recovery expenses.[74]

When officials choose not to pay a ransom and it costs their entity enormously higher sums of money to recover, some wonder if these officials should be legally responsible for their decision not to pay. However, such a question goes against the popular notion to never pay a ransom. Support for this viewpoint is growing; in 2019, more than 225 U.S. mayors at the U.S. Conference of Mayors signed a pledge promising not to pay a ransom if attacked.[75] The promise was made in hope of disincentivizing attackers, which is commonly thought as the best way to reduce attacks long-term. The logic follows that if attackers are no longer receiving ransom payments, they do not have a reason to initiate attacks in the first place. As this theory continues to gain popularity, it may be unlikely that officials who put the logic to the test by not paying a ransom would be responsible for the aftermath.

Another reason to support officials who do not pay ransoms is that nearly 33 percent of victims who pay a ransom are still never given a decryption key.[76] For these victims who elect to pay and still have to go through the entire cleanup process, the amount paid in ransom is yet another costly loss. In the end, it is unrealistic that city officials or company leaders who elect not to pay a ransom could be held liable for their decision.

---

[74] Lily Hay Newman, *Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare*, WIRED, (Apr. 23, 2018), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.
[75] *2019 Adopted Resolutions*, THE UNITED STATES CONFERENCE OF MAYORS, http://legacy.usmayors.org/resolutions/87th_Conference/proposedcommittee-preview.asp?committee=Criminal%2 0and%20Social%20Justice (last visited May 5, 2020).
[76] *Supra*, note 68.

Still, there is another line of questioning which asks whether officials can be found liable post-attack. If an official negligently operated an entity, thus leaving it susceptible to a ransomware attack or unable to recover in a time-efficient manner, could the official be held liable? For example, could officials who have control over approving, budgeting, and funding ransomware prevention tactics—yet do not implement these precautionary measures—be viewed as negligently disregarding their duties?[77]

Such was the case in early 2020, when the city and county governments of Durham, North Carolina were hit with synchronized ransomware attacks.[78] The attacks led some experts, such as CISO Ian Thorton-Trump,[79] to question if municipalities are doing enough to protect themselves from ransomware attacks. Thorton-Trump explained that it is extremely common for municipalities to put IT services and IT security "way down on the list of priorities for funding."[80] The end result is a department running old software on old computers with little-to-no security measures or backup procedures. Ultimately, this begs the question of whether officials who approve budgets that put their municipality or organization in such a position should be held liable for any personal constituent data that is lost, or for any hefty clean-up bills resulting from a ransomware attack. The question remains unanswered and lays the foundation for potential lawsuits against officials in years to come.

---

[77] Dan Lohrmann, *Who's to Blame or Not to Blame in Baltimore Attack*, GOVTECH, (June 2, 2019), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/ransomware-to-blame-or-not-to-blame.html.
[78] The attacks took place on Friday, March 6, 2020, and involved *Ryuk* malware. It is suspected the attackers belonged to a Russian hacking group, according to the North Carolina State Bureau of Investigations. *See* Lucas Ropek. Ransomware Attack Hits North Carolina City, County Governments, GOVTECH, (March 9, 2020), https://www.govtech.com/security/Ransomware-Attack-Hits-North-Carolina-City-County-Governments.html.
[79] Mr. Thornton-Trump is the Chief Information Security Officer of Cjyax, a company that provides cyber threat services. *See* Davey Winder, *Two 'Russian' Ransomware Attacks Take Down North Carolina City and County Government Systems*, FORBES, (March 10, 2020), https://www.forbes.com/sites/daveywinder/2020/03/10/two-russian-ransomware-attacks-take-down-north-carolina-city-and-county-government-systems/#24196605588f.
[80] *Id.*

Policy Implications

After companies and municipalities are hit with ransomware, it is understandable why they want to hold someone responsible for the attack. If attackers cannot be located, which is usually the case, then it is natural to look to other actors who could be liable in some way. However, holding most of the aforementioned actors liable after a ransomware attack would involve going down a slippery slope into a victim-blaming mentality. This is especially concerning when blaming IT professionals or low-level employees for systems being infected with malware. Firing the employees or holding them legally liable for the attack poses not only a deep-pocket concern, but an ethical quandary as well.

Holding these actors liable does very little but shift the blame away from the actual attackers to those who do not have the training, expertise, or budget to stay properly protected from these attacks. Instead of spending time and resources holding these actors responsible, cities should focus their attention on allocating proper funds to cybersecurity measures, such as hiring IT professionals who are proficient in ransomware prevention, and moving all data to cloud-based backup systems.

Just as in Lake City, Florida, some municipalities may fire an IT specialist for negligence after a ransomware attack to deter future employees from making the same decisions. The idea hinges on the age-old (and controversial) crime-prevention principle of deterrence. In a ransomware case, deterrence works by providing a severe punishment for those whose alleged negligence left an entity susceptible to attack or unable to cleanup efficiently post-attack. Future IT specialists, third-party vendors, employees, city officials, and other actors will choose not to make the same choices as their punished counterparts. It sounds like a sensical solution, but

practically speaking, deterrence is an antiquated concept with waning reliability.[81] Psychologists and criminal justice experts alike have performed countless experiments regarding deterrence and looked at statistics coming out of the U.S. carceral system.[82] Unsurprisingly, 70 percent of imprisoned persons reoffend within five years of leaving prison.[83] As such, filing civil suits for negligence against shallow-pocketed individuals or firing said individuals seems to rest almost exclusively on the idea of deterrence actually having a notable effect on future conduct. Because it does not, finding these actors liable for negligence is unlikely to do anything to reduce the number of ransomware attacks in this country.

Finally, it is also critical to remember there is a fine line between ignoring best practices and *truly* being negligent. At the end of the day, best practices are merely suggestions that companies and municipalities should take. Importantly, best practices are not obligations. Many practices, such as implementing user-based trainings, moving to cloud-based storage systems, obtaining cyber insurance, and having the latest versions of software are not possible without proper funding. Trying to place the blame on budget creators for not allocating enough funds for ransomware prevention or insurance would be a long and costly battle. And, most importantly, shifts the blame from ransomware attackers to their victims.

Conclusion

Finding actors liable after a ransomware attack is a messy, interconnected web that is far more complex than a simple "blame-game." In a tort liability action, many actors simultaneously face some degree of liability. This makes it next to impossible to find anyone legally responsible,

---

[81] *Loren Thompson*, What If Deterrence Doesn't Work Anymore? Five Reasons to Worry, FORBES, (Aug. 18, 2014), https://www.forbes.com/sites/lorenthompson/2014/08/18/what-if-deterrence-doesnt-work-anymore-five-reasons-to-worry/#5e132866be89.
[82] William R. Kelly, *Why Punishment Doesn't Reduce Crime*, PSYCHOLOGY TODAY, (Apr. 24, 2018), https://www.psychologytoday.com/us/blog/crime-and-punishment/201804/why-punishment-doesnt-reduce-crime.
[83] *Id*.

especially in internet-based attacks.[84] Even if certain actors seem more liable than others and litigation is pursuable, such cases may be unwise from a policy standpoint. Specifically, lawsuits hinging on victim-blaming mentalities are counterproductive in the effort to stop ransomware attackers, as the attackers are the main actors who should be responsible. Firing low-level employees or IT specialists without sound cause in hopes of deterring future action is also unlikely to work, as deterrence is a highly disproven theory in reducing the recidivism of unwanted actions.

Trying to blame other actors when the main culprit is not locatable is not a new phenomenon. In actions involving gun control and military weapons falling into the wrong hands, similar "blame-games" occur and lead to the type of messy litigation ransomware liability suits would likely cause.[85] At the end of the day, it is natural for a victim to want someone to blame after an attack. Nevertheless, acting out of emotion and holding other actors responsible for the actions of the actual attacker is likely to be a waste of time and effort. Assigning liability to other actors shifts the blame off the true attackers, who continue to face little-to-no repercussions for their actions. There is no reality where ransomware ceases to exist until actors work together to disincentivize attackers, which is next to impossible if legal responsibility shifts from said attackers to their victims.

[84] *Rasch*, at 3.
[85] *Supra*, note 77, at 2.