LEGISLATIVE REFERENCE BUREAU

Ransomware Attacks: Lessons for Wisconsin State and Local Government

Staci Duros, PHD
legislative analyst

Alex Rosenberg
legislative analyst

WISCONSIN POLICY PROJECT • February 2020, Volume 3, Number 3

One East Main Street, Suite 200, Madison, Wisconsin 53703
http://legis.wisconsin.gov/lrb • 608-504-5801

Introduction

According to a report from security software company Emsisoft, the United States "was hit by an unprecedented and unrelenting barrage of ransomware attacks" in 2019 that affected at least "113 state and municipal governments and agencies, 764 health care providers, 89 universities, colleges, and school districts with operations at up to 1,233 individual schools potentially affected." The cost of these attacks is in excess of $7.5 billion.[1] In May 2019, the City of Baltimore suffered a ransomware attack that disrupted the city's ability to process utility and real estate transactions, as well as the city's government email, phone systems, and other services.[2] While the city refused to pay the ransom demand of $76,000, recovery costs have been estimated at more than $18 million.[3] Similarly, a widespread, coordinated ransomware attack compromised computer systems in 22 small towns in Texas, delaying more than 1,000 home sales, disabling the website that utility customers use to pay water bills, derailing city voicemail and email systems, disrupting a database for parking fines, and prompting the cancellation of city council hearings.[4] At least two municipalities in Florida confronted ransomware attacks and ended up spending around $1.1 million combined to recover.[5] Less than a month later, the judicial system of Georgia became another victim of an attack.[6]

Closer to home, the Wisconsin cities of Racine and Oshkosh recently faced ransomware attacks just days apart.[7] Oshkosh residents had to pay their utility bills either through the mail or in person at city hall (and receive a handwritten note as a receipt). They also had to pay their tax bills, which were due the very same week of the attack, at designated financial institutions.[8]

[1] Emsisoft Malware Lab, The State of Ransomware in the US: Report and Statistics 2019, (Emsisoft revised December 31, 2019), https://blog.emsisoft.com. Emsisoft adds that their $7.5 billion "overstates the actual costs—a small school district's recovery expenses are unlikely to run to seven figures—it nonetheless provides an indication of the enormous financial impact of these incidents."

[2] Sean Gallagher, "Baltimore Ransomware Nightmare Could Last Weeks More, with Big Consequences," *Ars Technica*, May 20, 2019, https://arstechnica.com.

[3] Ian Duncan, "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts," *Baltimore Sun*, May 29, 2019, https://baltimoresun.com.

[4] Tim Starks, "Washington Idle as Ransomware Ravages Cities Big and Small," *Politico*, September 28, 2019, https://politico.com; Manny Fernandez, Mihir Zaveri, and Emily S. Rueb, "Ransomware Attack Hits 22 Texas Towns, Authorities Say," *New York Times*, August 20, 2019, https://nytimes.com.

[5] Riviera Beach agreed to pay $600,000 to restore its encrypted systems and is reported to be spending over $1 million to replace or restore its systems; the City of Lake City's insurance provider paid around $500,000 in Bitcoin. Key Biscayne, FL, officially reported that it suffered "a data security event," not revealing the nature of the incident or if it involved ransomware; see John Haughey, "Lake City Latest Florida Victim to Pay 'Ransomware' Hackers," *Center Square*, June 29, 2019, sunshinestatenews.com.

[6] Kaitlyn S. Ross and Jonathan Raymond, "Georgia Court System Hit By Ransomware Attack," *Atlanta WXIA-NBC*, July 1, 2019, https://11alive.com.

[7] Caitlin Sievers, "Ransomware Infects City of Racine Computer Systems," *Journal Times*, February 2, 2020, https://journaltimes.com; Monique Lopez, "Oshkosh Becomes One of Ransomware's Latest Victims," *WLUK*, January 30, 2020, https://fox11online.com.While authorities characterized these attacks as ransomware attacks, neither Racine nor Oshkosh has reported a ransom demand as of the date of this publication.

[8] Lopez, "Oshkosh Becomes One of Ransomware's Latest Victims."

Ransomware attacks on public entities are not just a costly inconvenience; the challenges these incidents present to health care providers can have an immediate and direct impact on patient care. In September 2019, Campbell County Health in Wyoming suffered a ransomware attack that forced the cancellation of patient surgeries and the transfer of emergency patients to alternative facilities, and halted new inpatient admissions.[9] Similarly, DCH Health Systems in Alabama faced a ransomware attack that stopped the admission of new patients to all of its hospitals and required that its medical staff use pen-and-paper records in place of digital records.[10]

Across the country, a number of public entities have found themselves grappling with high-profile ransomware attacks. This report provides a basic overview of ransomware and how ransomware attacks spread. Next, the report describes why local and state governments present an attractive target for ransomware attacks and the dilemma that they face on whether or not to pay the ransom. Then, the report reviews recommendations by cybersecurity and public policy experts on how local and state entities can recover from an attack or avoid one altogether. The report concludes with an examination of contemporary federal and state legislative efforts to address the rise of ransomware attacks.

Ransomware basics

Ransomware is malicious software (malware[11]) that prevents a victim from accessing some or all of the data on a computer until he or she pays a ransom. Whereas standard computer viruses merely damage, steal, or delete data, ransomware also includes (or attackers claim that it includes) a mechanism to undo the damage following a ransom payment. Typically, entities infected with ransomware are alerted to its presence only after user data has already been encrypted. While ransomware attacks have been around for at least the past three decades,[12] this type of cybercrime remained infrequent until the last decade or so.[13]

[9] "Service Disruptions at CCH; No ETA," Campbell County Health, September 20, 2019, https://cchwyo.org.

[10] Nathan Eddy, "Alabama Hospital System DCH Pays to Restore Systems after Ransomware Attack," *Healthcare IT News*, October 7, 2019, https://healthcareitnews.com. Four patients of DCH Health Systems have filed a federal class action lawsuit in response to the October attack; see Howard Koplowitz, "DCH Health System Patients File Federal Suit Over Ransomware Attack," *Tuscaloosa Real-Time News*, December 23, 2019, https://al.com.

[11] The term "malware" can refer to any program or file that is harmful to a computer (mobile device, tablet, etc.) user.

[12] The first documented ransomware attack occurred in 1989. Harvard biologist Dr. Joseph L. Popp mailed out 20,000 floppy disks to researchers in more than 90 countries ahead of the World Health Organization's AIDS conference. The floppy disk was labelled as the "AIDS Information Introductory Survey Diskette" and contained a survey program that analyzed an individual's risk of acquiring AIDS. However, buried in the code was a virus that became activated only after an infected computer was powered on 90 times. After this threshold was reached, the malware displayed a message on the victim's computer demanding a payment of $189. These payments were to be mailed to a P.O. Box in Panama. This ransomware attack became known as the AIDS Trojan, or the PC Cyborg.

[13] Cybersecurity and Infrastructure Security Agency (CISA), *CISA Insights: Ransomware Outbreak*, (August 2019), https://us-cert.gov; see also Muhammad Ubale Kiru and Aman B. Jantan, "The Age of Ransomware: Understanding Ransomware and Its Countermeasures," in Ryma Abassi (ed.), *Artificial Intelligence and Security Challenges in Emerging Networks*, (Pennsylvania: IGI Global, 2019), 1–37.

Ransomware spreads mostly through two types of attack strategies: social engineering techniques and exploitation of bugs in outdated software.[14] "Social engineering" refers to a broad range of techniques that lure victims into taking some form of compromising action. Tech support scams are the most common method of social engineering attacks.[15] In a tech support scam, a scammer pretends to be support staff from a software company such as Microsoft,[16] and contacts a victim either by calling with spoofed caller ID information or by tricking the victim into clicking a link or calling a phone number from a fake error message on a website. The scammer then instructs the victim to install supposedly helpful software that actually gives the scammer control over the computer, at which point the scammer can steal sensitive data and demand a ransom to restore access.

The second most common social engineering technique to deliver ransomware is through phishing, which tricks a victim into action through a message or call from a trustworthy source.[17] For example, a user might receive an email message that purports to be from his or her boss asking the employee to review a document attached in the email. As soon as the employee clicks on it, installation and execution of the ransomware begins. All it takes is one employee mistakenly clicking the wrong thing to allow ransomware attackers to cripple an entire system like the ransomware attack that recently occurred in Racine, Wisconsin. A City of Racine employee "clicked on a link in an email,"[18] unleashing a virus that sent all of the city's operations offline for weeks.[19] Likewise, in December 2019, a ransomware attack against the City of New Orleans was triggered by a city employee clicking on a phishing email.[20]

The other major method of attack exploits vulnerabilities of out-of-date software. All software has bugs, and sometimes an attacker can take advantage of a bug to gain illicit access to a computer system, often through automated malware programs that seek out and take over vulnerable systems. Responsible software companies, therefore, work as quickly as possible to release updates or patches to fix the bugs and eliminate vulnerabilities. However, usually the software on a system cannot be fully updated until someone takes an action such as restarting a computer. Even after a patch is available, attackers can still take over systems that have not been fully updated.

[14] "Story of the Year 2019: Cities under Ransomware Siege," Kaspersky, December 11, 2019, https://securelist.com.

[15] Tech support scams that exploit Remote Desktop Protocol (RDP) systems make up an estimated 57.4 percent of social engineering attacks; see Coveware, *Q4 Ransomware Marketplace Report: Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate*, (Westport, CT: Coveware, January 23, 2020), https://coveware.com .

[16] "Protect Yourself from Tech Support Scams," Microsoft, June 3, 2019, https://support.microsoft.com.

[17] Phishing makes up an estimated 26.3 percent of social engineering attacks; see Coveware, Q4 Ransomware Marketplace Report.

[18] Caitlin Sievers, "Ransomware Infects City of Racine Computer Systems," *Journal Times*, February 2, 2020, https://journaltimes.com.

[19] Jeff Ostrowski, "How a Riviera Beach Police Department Email That Shouldn't Have Been Opened Turned Disastrous for the City," *Palm Beach Post*, June 7, 2019, https://palmbeachpost.com.

[20] Sarah Wray, "New Orleans Cyber Attack Triggered by Phishing Email," *Smart Cities World*, December 23, 2019, https://smartcitiesworld.net.

The most prominent example of attackers exploiting ongoing vulnerabilities is WannaCry, an "all-time leader" in multiple rankings of the most prevalent pieces of malware.[21] WannaCry exploited a vulnerability in the networking components of Microsoft's Windows systems. WannaCry attacks began on May 12, 2017, and spread so rapidly that the ransomware encrypted data on 75,000 computers in less than one day.[22] Two months before the attack, Microsoft had released a security update to fix the vulnerability that WannaCry would go on to exploit.[23] The president of Microsoft, Brad Smith, stated that while the security patch "protected newer Windows systems and computers that had enabled Windows Update to apply this latest update, many computers remained unpatched globally. As a result, many hospitals, businesses, governments, and computers at homes were affected."[24] Smith added, "The fact that so many computers remained vulnerable two months after the release of a patch illustrates this aspect [the degree to which cybersecurity has become a shared responsibility between tech companies and customers]. As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems."

Had users updated their software on time, WannaCry would not have posed a threat. Even today, many users and organizations have yet to update their systems with the patches Microsoft made available in 2017; as of late 2019, WannaCry still represents more than a fifth of ransomware attacks.[25]

Targeting the public sector

PC Magazine described 2019 as "the year ransomware feasted on the U.S. public sector," as state and local government agencies, schools, and healthcare providers were among the most prevalent ransomware targets.[26] State and local governments have become attractive targets of ransomware attacks for several key reasons, such as lack of funding and workforce shortages.[27]

Public institutions often have computer systems that are easy to attack. Governments and schools with limited budgets tend not to keep up with all of the latest, often safer, technology trends. As a result, these institutions might be running older computers and software that do not have built-in protection for newer and more sophisticated malware

[21] "Story of the Year 2019," Kaspersky.

[22] "Cyber-Attack: Europol Says It Was Unprecedented in Scale," *BBC News*, May 13, 2017, https://bbc.com.

[23] Brad Smith, "The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack," *The Official Microsoft Blog*, May 14, 2017, https://blogs.microsoft.com.

[24] Brad Smith, "The Need for Urgent Collective Action to Keep People Safe Online."

[25] "Story of the Year 2019," Kaspersky.

[26] Michael Kan, "2019: The Year Ransomware Feasted on the US Public Sector," *PC Magazine*, December 13, 2019, https://www.pcmag.com.

[27] Srini Subramanian and Doug Robinson, 2018 Deloitte-NASCIO Cybersecurity Study—States at Risk: Bold Plays for Change, (National Association of State Chief Information Officers (NASCIO) and Deloitte, October 2018), https://nascio.org.

threats. Rigorous security processes could mitigate much of the risk of the older systems, but public entities often spend less than the commercial sector on the IT staff that would implement those processes.

Even when governments do budget for cybersecurity, Kaspersky reports, "the cybersecurity budgeting of municipalities is often more focused on insurance and emergency response than on proactive defense measures."[28] As a result, when attacked, "the only possible solution is to pay the criminals and facilitate their activities."[29]

A second reason for governments' vulnerability to ransomware is that governments face significant pressures to pay ransoms. Ransomware attacks can disrupt all citizen-facing services and operations, including libraries, law enforcement agencies, school districts, court systems, emergency services, municipal governments, and state-level agencies and departments.[30] Government systems support essential public services, so there is likely to be immediate public demand for systems to be restored after an attack. Even managed service providers (MSPs), private companies that handle IT systems for local governments and medical clinics, are not immune.[31] When these systems go down, there can be serious public safety risks until they are restored. As a result, public entities might feel even more pressure to quickly pay ransoms.

To pay, or not to pay

Unlike the band Radiohead, which decided to release its ransomed music instead of succumbing to extortion attempts, local and state entities faced with a ransomware attack have no similar recourse. Local and state governments either have to pay or deal with the aftermath.

However, both cybersecurity experts and law enforcement officials recommend that ransomware victims avoid paying ransoms. Data-loss prevention firm Digital Guardian states that "paying the ransom only establishes you as a paying target for future attacks

[28] "Story of the Year 2019," Kaspersky.

[29] "Story of the Year 2019," Kaspersky.

[30] For example, Spartanburg County Library in South Carolina, see Jenni Mathews, "Spartanburg Co. Libraries Hit By Ransomware Attack," *WSPA News*, January 31, 2018, https://wspa.com; Salisbury Police Department in Maryland, see Brooke Reese, "Salisbury Police Department Faces 'Worst Computer Network Attack' In History," *WBOC News*, January 23, 2019, https://wboc.com; Forsyth Public Schools in Montana, see Kayla Elliot, "Forsyth Public Schools Overrun with Malware," *TechTalk*, April 3, 2017, https://techtalk.pcmatic.com; Connecticut Judicial Branch, see David Owens, "Ransomware Attack Takes Down State Court Computers," *Hartford Courant*, March 9, 2018, http://courant/com; Henry County 911 in Tennessee, see Glenn Tanner, "Paris TN: 911 Director Archer Confirms Ransomware Hack from Last Year," *Paris Post-Intelligencer*, July 19, 2017, https://parispi.net; the City of Atlanta, Georgia, see Theo Douglas, "Nearly Two Weeks Post-Cyberattack, Atlanta Continues its Recovery," *GovermentTechnology*, April 4, 2018, https://govtech.com; Colorado Department of Transportation, see Jaclyn Allen, "CDOT Employees Dealing with Yet Another Samsam Ransomware Attack," *ABC News 7 Denver*, March 1, 2018, https://thedenverchannel.com.

[31] MSPs may in some cases make their clients more vulnerable by providing another entry point for attackers. For example, the Louisiana secretary of state blames MSPs for several recent attacks in the state; see Edward Gately, "MSPs Blasted for Bad Cybersecurity Practices," *Channel Futures*, February 6, 2020, https://www.channelfutures.com; Renee Dudley, "The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once," *ProPublica*, September 12, 2019, https://propublica.org.

and has even led to follow-on data breaches at some organizations. Unless you have absolutely no other choice, avoid paying ransoms."[32] Similarly, the FBI "does not support paying a ransom in response to a ransomware attack" both because "paying a ransom doesn't guarantee an organization that it will get its data back" and because "paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity."[33]

According to a sweeping ProPublica report, insurance companies that cover ransomware attacks often prefer to pay the ransoms for their clients rather than pay to undertake recovery efforts.[34] ProPublica found that insurers "often accommodate attackers' demands, even when alternatives such as saved backup files may be available."[35] In the case of Baltimore, for example, the actual costs to recover and restore systems totaled over $18 million, which far exceeded the attackers' ransom demand of $76,000. As a result, insurers can cut costs by simply paying attackers. In fact, two of the Florida cities that were affected by the 2019 attacks—Lake City and Riviera Beach—decided to authorize their insurance carrier to pay since the cities had policies that covered the majority of the ransom amounts—$460,000 and $600,000, respectively—while the cities were responsible only for $10,000 deductibles.[36] Lake City Mayor Stephen Witt stated that he preferred to have the city's insurance carrier pay the ransom: "We pay a $10,000 deductible, and we get back to business, hopefully. Or we go, 'No, we're not going to do that,' then we spend money we don't have to just get back up and running. And so to me, it wasn't a pleasant decision, but it was the only decision."[37]

The tendency for insurance carriers to pay may drive the profitability of cyber-insurance policies. Professional services firm Aon reports that as of 2018, the average "loss ratio" for cyber-insurance was 35.4 percent—that is, insurers paid out an average of 35.4 cents in claims for every dollar they collected on cyber insurance premiums.[38] Claims paid out for other insurance products are a more significant cost to the insurers; the National Association of Insurance Commissioners reports that the average loss ratio across all insurance lines of business was about 61.6 percent in 2018.[39] Thus, ransomware insurance carriers can create a vicious cycle that incentivizes more attacks and higher

[32] "Ransomware Protection: Best Practices, Tips, and Solutions," *Digital Guardian*, October 3, 2016, https://digitalguardian.com.

[33] "Cyber Crime," Federal Bureau of Investigation (FBI), accessed June 25, 2019, https://www.fbi.gov.

[34] Renee Dudley, "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," *ProPublica*, August 27, 2019, https://www.propublica.org.

[35] Dudley, "The Extortion Economy."

[36] Andrew Caplan, "Lake City, Fla., Authorizes Nearly $500k Ransomware Payment," June 26, 2019, https://govtech.com; Tony Doris, "Why Riviera Beach Agreed to Pay $600,000 Ransom Payment to Regain Data Access…and Will It Work?," *Palm Beach Post*, June 20, 2019, https://palmbeachpost.com.

[37] Dudley, "The Extortion Economy."

[38] Aon, US Cyber Market Update, (Aon, June 2019), http://thoughtleadership.aon.com.

[39] National Association of Insurance Commissioners, 2018 Market Share Reports for Property/Casualty Groups and Companies By State and Countrywide, (National Association of Insurance Commissioners, 2019), https://naic.org.

payments. ProPublica summarizes input from the FBI and a range of cybersecurity researchers:

> [When insurers pay ransoms,] it holds down claim costs by avoiding expenses such as covering lost . . . and ongoing fees for consultants aiding in data recovery. And, by rewarding hackers, it encourages more ransomware attacks, which in turn frighten more businesses and government agencies into buying policies.[40]

Ransomware attackers continue to profit from easy payouts, and insurers profit from increased demand for ransomware policies. In fact, recent data show that average ransom demands are growing faster than ever, and may have more than doubled in the last three months of 2019 alone.[41] In the absence of legislation or other significant changes to the existing incentive structure, this cycle is likely to continue.

For organizations that have fallen victim to ransomware, experts in law enforcement and cybersecurity recommend the following recovery tasks rather than paying ransoms:[42]

- Identify infected devices and immediately remove them from the network.
- Notify law enforcement authorities that the attack has taken place. In the United States, the FBI and the Secret Service are appropriate agencies to contact.
- Notify employees, customers, and other stakeholders that data may have been compromised.
- Patch and update security for all systems, including changing passwords or other credentials for accounts that may have been compromised.
- Restore data from backups only after all security updates are complete·[43]

How to defend against ransomware

Although banks would be valuable ransomware targets, they have, in general, implemented cybersecurity best practices so well that not a single bank disclosed a ransomware incident in 2019.[44] However, state and local governments and other public entities are not defending themselves to the same level. Cybersecurity firm Veritas released the

[40] Dudley, "The Extortion Economy."

[41] Coveware, "Q4 Ransomware Marketplace Report."

[42] Adapted from government and industry resources including Federal Bureau of Investigation, "Ransomware Prevention and Response for CEOs," accessed February 10, 2020, https://www.fbi.gov; Federal Bureau of Investigation et. al., "Ransomware Prevention and Response for CISOs," accessed February 10, 2020, https://www.fbi.gov; "Story of the Year 2019," Kaspersky; Christina Mercer and Charlotte Trueman, "How to Properly Respond to a Ransomware Attack," *CIO*, March 5, 2019, https://www.cio.com; "Ransomware Threats: Is Your Agency Ready?," Veritas, December 2019, https://www.fedscoop.com; Melissa J. Krasnow, "Guidance on Ransomware," International Risk Management Institute, Inc., January 2017, https://www.irmi.com.

[43] In addition to the organization's own backups, other resources such as the No More Ransom project are available to help organizations recover from ransomware without paying the ransom. The No More Ransom project is a collaboration between Europol, the Dutch National Police, Kaspersky Lab, and McAfee that provides victims of a ransomware infection with decryption tools to remove ransomware for more than 80 ransomware variants.

[44] Emsisoft Malware Lab, "The State of Ransomware in the US."

results of a survey of federal and state government agencies in which only about half of the respondents reported having procedures to recover or isolate ransomed data, and "far fewer" had any plans to engage with law enforcement and cybersecurity specialists following a ransomware attack.[45] Veritas states that "agencies could use more help not only to identify appropriate detection and response technologies, but also in creating appropriate response procedures in the event of an attack."[46] Emsisoft agrees with this sentiment, arguing that "cybersecurity is complex and getting it right can be challenging, especially for smaller organizations." For this reason, state-mandated standards for security practices can encourage public entities to devote their resources to meeting clearly defined requirements.[47]

Cybersecurity is complex, but the first steps to bolstering defenses against ransomware and similar attacks are relatively simple. A joint statement by the Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) distills the basics down to three steps:[48]

1. Back up critical systems on an automatic, regular schedule.
2. Train all employees to recognize, avoid, and report cybersecurity incidents and threats.
3. Update and regularly review cybersecurity incident response plans to account for ransomware attacks and other new threats.

Organizations such as small government entities that do not have a substantial in-house information technology staff can take advantage of resources that aim to centralize cybersecurity expertise. For example, the MS-ISAC provides mission-critical services, such as two-way sharing, as a central resource on cyber threats.[49] Organizations can become members and have access to resources such as 24/7 security operation and incident response services, cybersecurity advisories, and access to secure portals and awareness or education materials. These services can be beneficial for local governments looking to advance their cybersecurity.

Additional resources are forthcoming from the National Institute of Standards and Technology (NIST), a non-regulatory federal agency. NIST has released a draft set of policy and technical documents on the topic of ransomware referred to as *Cybersecurity Special Publication 1800-25, Identifying and Protecting Assets Against Ransomware and*

[45] "Ransomware Threats", Veritas.

[46] "Ransomware Threats", Veritas.

[47] Emsisoft Malware Lab, "The State of Ransomware in the US."

[48] Cybersecurity and Infrastructure Security Agency (CISA) et al., "CISA, MS-IAC, NGA & NASCIO Recommend Immediate Action to Safeguard Against Ransomware Attacks," (CISA, MS-IAC, NGA & NASCIO, July 29, 2019), https://www.us-cert.gov.

[49] "CIS SecureSuite Membership," Center for Internet Security, accessed February 10, 2020, https://www.cisecurity.org.

Other Destructive Events. NIST publishes and supplies standards and standardized reference manuals that are used commercially and incorporated into laws and regulations. The Wisconsin Administrative Code, for example, includes dozens of references to NIST standards.[50] The new NIST ransomware documents could similarly serve as standardized references in state and federal laws.

State and local government legislation can also provide significant guidance and resources for public entities facing the threat of ransomware. States' efforts in this area are described in the following section.

Legal cases

Because ransomware is a relatively new phenomenon, the legal landscape surrounding ransomware attacks is far from settled. One of the earliest high-profile lawsuits related to ransomware was a class action suit against Allscripts Healthcare Solutions, a major vendor of electronic health record software, by customers who lost access to their electronic health records following a ransomware attack on Allscripts. The class action suit was dismissed over a distinction between the parent company toward which the lawsuit was directed and the subsidiary that was responsible for cybersecurity, leaving substantive legal questions over damages and responsibility unresolved.[51]

There are a few earlier cases, however, in a similar vein. In a 2017 case, a Rhode Island law firm sued its insurer for $700,000 in lost business following a ransomware attack. The insurer claimed it had no legal obligation to cover ransomware losses beyond the policy maximum of $20,000 for losses caused by computer viruses, and that policy coverage for lost business income applied only in situations involving physical loss or damage to property at the business premises. The case was settled with undisclosed terms in 2018.[52] In a more decisive case, both a district court and a court of appeals ruled that a ransomware attack against Medidata Solutions Inc. did fall under existing computer fraud provisions of its insurance coverage.[53] As ransomware and cyber insurance policies both become more prevalent, there will no doubt be many more cases like these.

There have been a number of court cases in which ransomware is not a central issue but comes up because a participant in the case has suffered a ransomware attack that affects documents or data relevant to the case. For example, in September 2019, a district court in California ruled that because a ransomware attack contributed to a delay in

[50] See, for example, Wis. Admin. Code ATCP § 91.03 (1) (e), Wis. Admin. Code DHS § 159.32 (8) (g) 4., and Wis. Admin. Code NR § 149.45 (1) (b).

[51] Jackie Drees, "Cybersecurity Lawsuit against Allscripts Tossed by Judge," *Becker's Health IT & CIO Report*, June 6, 2019, https://www.beckershospitalreview.com.

[52] Jason Tashea, "Are You Covered? Cyber Insurance Market Is Highly Unstable and Lacks Uniformity," *ABA Journal*, June 1, 2018, http://www.abajournal.com.

[53] Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117 (2d Cir. 2018).

producing required documents, the defendant had not negligently destroyed or altered the documents.[54] By and large, courts do not appear to treat ransomware differently than other factors that contribute to issues with maintaining or providing documents, and are adjudicating these issues on the basis of existing legal standards.

Federal action on ransomware

Ransomware is a crime that has significant regulatory implications and can involve important legal responsibilities and liabilities. At a minimum, ransomware schemes run afoul of the federal computer crime statute,[55] which forbids hacking with intent to extort something of value from the victim. Federal law also criminalizes acts such as computer fraud and destruction of electronic property,[56] extortion,[57] threats,[58] or threats of violence to property.[59]

A federal spending bill passed at the end of 2019 included provisions that require the Department of Homeland Security to maintain "cyber hunt and incident response teams" tasked with assisting both public entities and the private sector with identifying cybersecurity risks, protecting against those risks, and recovering from cyber incidents. The teams will also publish "recommendations . . . for improving overall network and control systems security to lower cybersecurity risks."[60]

State and local action on ransomware

In late November 2019, Louisiana Governor John Bel Edwards declared a state of emergency following a ransomware attack that affected the state's computer network.[61] The state of emergency declaration allowed state agencies to coordinate their response with federal and local entities[62] to preserve data confidentiality and security.[63] This incident was the second time that Governor Edwards declared a state of emergency due to ransom-

[54] Trepco Imps. & Distribution, Ltd. v. Ariz. Bevs. USA, LLC, No. ED CV 18-2605-JGB (SPx), 2019 U.S. Dist. LEXIS 220085 (C.D. Cal. Sep. 12, 2019).

[55] 18 U.S.C. § 1030, and particularly subsection (a) (7).

[56] 18 U.S.C. § 1030 (a).

[57] 18 U.S.C. § 873.

[58] 18 U.S.C. § 875.

[59] 18 U.S.C. § 1951.

[60] H.R. 1865, the Further Consolidated Appropriations Act, 2020, includes the DHS Cyber Hunt and Incident Response Teams Act of 2019, which had previously been introduced and gone through committee as a standalone bill in the senate (S. 315).

[61] Paul Murphy, "Governor Declares State of Emergency after Ransomware Attack on Louisiana," *WWL-TV News New Orleans*, November 22, 2019, https://wwltv.com; Governor John Bel Edwards, Proclamation Number 173 JBE 2019, (November 22, 2019).

[62] Among the larger agencies that are mobilized to assist through an emergency declaration are the FBI, the Louisiana Office of Technology Services, the Louisiana State Police, the Louisiana National Guard, and the Governor's Office of Homeland Security Emergency Preparedness (GOHSEP).

[63] Governor John Bel Edwards, Proclamation Number 173 JBE 2019, (November 22, 2019), sections 6–8.

ware attack,[64] and Louisiana was the second of three states to respond to cyberattacks with a statewide emergency.[65]

Few states have taken similarly significant legislative action directly related to ransomware. There are only five states—California, Connecticut, Michigan, Texas, and Wyoming—that explicitly name ransomware or computer extortion or both in their statutes:

- **California:** Cal. Penal Code § 523 (2017) (2015 S.B. 1137) defines ransomware in state law and makes introducing ransomware into a computer punishable "as if [the property of a person] were actually obtained by means of the ransomware."
- **Connecticut:** Conn. Gen. Stat. § 53a-262 (2019) (2017 H.B. 7304) defines ransomware in state law and makes extortion by use of ransomware a state class E felony punishable by imprisonment up to three years.
- **Michigan:** Mich. Comp. Laws §§ 750.409b and 777.16t (2020) (2017 H.B. 5257 and 2017 H.B. 5258) define ransomware in state law and make possession of ransomware with the intent to use it a felony punishable by imprisonment up to three years.
- **Texas:** Tex. Penal Code Ann. § 33.023 (2019) (2017 H.B. 9) defines ransomware in state law and includes intentional introduction of ransomware among a number of new cybercrime-related criminal offenses with penalties that correspond to dollar amounts involved.
- **Wyoming:** Wyo. Stat. §§ 6-3-506 and 6-3-507 (2019) (2017 S.F. 0033) define ransomware in state law and make computer extortion a felony punishable by imprisonment up to 10 years, a fine up to $10,000, or both.

New York is currently considering legislation that bans municipalities from paying ransoms following a cyberattack. 2019 New York Senate Bill S7246 was introduced in mid-January 2020 and, as of early February, has not yet received a committee hearing or vote.

There do not yet appear to be any instances of states enacting statutory caps or bans on ransom payments or other similar legislation suggested by cybersecurity experts.

In addition to ransomware-specific law, states' laws related to data breaches can also apply to ransomware attacks. For example, Wis. Stat. § 134.98 sets notification requirements for entities that have been subject to a data breach. Since some ransomware attacks involve the acquisition or potential acquisition of personal data by the attacker, breached entities could be required to issue notifications about ransomware attacks just like other

[64] Governor John Bel Edwards, Proclamation Number 155 JBE 2019, (July 23, 2019). This emergency declaration was in response to several ransomware attacks against school districts across the state of Louisiana and represented the first activation of the state's emergency response to a cybersecurity incident. See also Benjamin Freed, "Emergency Declarations Improve Cyberattack Recovery, Report Says," *Statescoop*, August 8, 2019, https://statescoop.com.

[65] The three states are Colorado (March 1, 2018), Louisiana (July 23, 2019, and November 22, 2019), and Texas (August 16, 2019). Texas's declaration differs from the states of Colorado and Louisiana because Texas passed legislation in 2017 to allow for the same type of coordination the other two states achieved by emergency declaration (2017 H.B. 8, Tex. Gov't. Code § 2054.518).

data breaches.[66] Similarly, state-mandated cybersecurity plans and practices might apply to ransomware, even if ransomware is not specifically named in the statutes. However, state mandates in this area may need to be re-examined and updated to account for ransomware and other new online threats.

Ransomware has also caught the attention of the United States Conference of Mayors, which passed a non-binding resolution in July 2019 that called on cities to "stand united against paying ransoms in the event of an IT security breach."[67] However, John Zanni, CEO of cybersecurity company Acronis SCS, argued that while he agreed with the sentiment of the resolution, he argued that "ultimately it will have zero impact. Ransomware attackers have now gotten a taste for attacking state and local government. They've found honeypots of opportunity and they're not going to stop."[68]

Conclusion

Experts agree that ransomware attacks are growing in prevalence and that local and state government entities are particularly vulnerable and valuable targets for attackers. Because ransomware attacks against public entities has proven to be lucrative to criminal enterprises, the public sector should expect ransomware attacks to increase in frequency and in sophistication. By and large, financial incentives point public entities toward purchasing cyber insurance and paying ransoms when attacked in order to quickly restore functionality of their systems. However, these same incentives lead to a vicious cycle of more attacks, higher ransom demands, higher insurance premiums, and higher payouts to criminal attackers. While few states have enacted legislation that specifically targets ransomware, this is a policy area in which both federal and state legislation could effectively reshape the existing incentive structure and reduce both the prevalence and profitability of ransomware attacks. ■

[66] For more information about data breaches and related legislation, see Alex Rosenberg, "Data Breaches: Risk, Recovery, and Regulation," *Wisconsin Policy Project* 2, no. 4 (Madison, WI: Legislative Reference Bureau, 2019), https://docs.legis.wisconsin.gov.

[67] "87th Annual Meeting: Opposing Payment to Ransomware Attack Perpetrators," The United States Conference of Mayors, July 2019, https://usmayors.org.

[68] Colin Wood, "Mayors Pass Resolution Against Paying Ransomware Ransoms," *StateScoop*, July 10, 2019, https://statescoop.com.