SEPTEMBER 2022

# Hard Choices in a Ransomware Attack

AUTHORS
Emily Harding
Harshana Ghoorhoo

A Report of the CSIS International Security Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SEPTEMBER 2022

# Hard Choices in a Ransomare Attack

AUTHORS
Emily Harding
Harshana Ghoorhoo

A Report of the CSIS International Security Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

# About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

**© 2022 by the Center for Strategic and International Studies. All rights reserved.**

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

# Acknowledgments

This report is made possible by project support from Microsoft Inc. The author would like to thank Anuj Goel, Michael Daniel, Atiim Phillips, and Seth Walton for their insightful feedback. Any errors or omissions are solely the responsibility of the author. Analysis and graphs are based on collected data; the author welcomes recommendations of relevant data sets for future analysis on this subject.

# Contents


**1 | The Core Issue** **1**

**2 | Background on Ransomware Attacks** **3**

**3 | A Crisis Spurs Hard Questions** **5**

*The Attacks* *6*

*The Call* *7*

*The Insurance Policy* *7*

*The Status of Backups* *8*

*The First Responders: Forensics and Incident Response* *9*

*The Communication Strategy* *10*

*The Long Recovery* *11*

*The Federal Authorities* *12*

*To Pay or Not to Pay* *13*

*Final Results* *14*

**4 | Findings** **16**

**5 | Recommendations** **19**

**6 | Conclusion** **23**

**About the Authors** **24**

**Endnotes** **26**

1

# The Core Issue

## A Policy Priority

Ransomware attacks started as a novelty but have now become a clear and present danger to entities of every size and function. The number of ransomware attacks and the price of demanded ransoms have escalated steeply since 2018.

Legislation and policy have not kept up. Policymakers have discussed taking basic steps, such as educating the public about multifactor authentication, and extreme steps, such as outlawing ransom payments. The Biden administration has devoted effort and imposed urgency on cybersecurity improvements, including issuing Executive Order 14028 in May 2021 and working with the G7 and other allies and partners to combat cybercrime.[1] The judicial system has attempted to do its part: the first indictment of a ransomware actor was in November 2018 when the Department of Justice (DOJ) charged two Iranian nationals with deploying ransomware to extort numerous entities, including hospitals.[2] Four years later, in mid-August 2022, the DOJ announced a rare success: extradition of a Russian national suspected of laundering cryptocurrency for ransomware gangs, who had unwisely wandered into a country friendly to the United States.[3] Despite these major steps forward, this approach has not proven to be effective for either punishment or deterrence.

Creating a smart policy about a newly emerged, technical subject is immensely challenging. Policymakers have sought to shape the incentive structure for victims to incentivize defense and disincentivize ransom payments. While they are sympathetic to businesses who fall victim to these attacks, which can sometimes be existentially threatening, few policymakers (or their staff) have ever experienced the shock of an attack firsthand and, as a result, are searching with incomplete information for the right combination of carrots and sticks that will help victims and hurt attackers. This project aims to illuminate a path forward.

Many entities could also benefit from imagining themselves in the victim's shoes. Whether due to a lack of resources, a lack of knowledge, or a misplaced sense of optimism that it will not happen to them, some entities have not yet taken the security steps needed to protect themselves. In particular, utilities, schools, and municipalities have out-of-date software and lack the funds for effective defense, cyber insurance, or protection from top cybersecurity firms. This project can also help alert those entities to the difficult realities of an attack.

***Few policymakers or their staff have ever experienced the shock of an attack firsthand and, as a result, are searching with incomplete information for the right combination of carrots and sticks that will help victims and hurt attackers.***

2

# Background on Ransomware Attacks

The raw numbers on ransomware attacks and ransom payouts are striking. While accurate data is notoriously difficult to find in this space, given inconsistent reporting, the scale and trend lines are notable:

- In a 2021 survey of critical infrastructure entities, 80 percent reported experiencing a ransomware attack in the last year.[4]
- One cybersecurity firm estimated there were 623 million attempted ransomware attacks worldwide in 2021 alone—an average of 20 every second.
- With the growing rate of ransomware attacks has come a high incidence of ransomware payments. Financial organizations reported $590 million in ransomware payments during only the first half of 2021, a 42 percent increase from 2020.[5]
- By 2020, the average ransom payment was over $200,000, forcing some cyber-insurance companies out of the market.[6]
- While estimates vary, an IBM report found that the average total cost of a ransomware attack for an entity is $4.6 million, based on a survey of 500 organizations worldwide.[7]

Victims such as hospitals, financial services, and universities must balance an additional potential cost: leaks of customer data. Given the sensitive nature of their customers' data, such victims often fear data leaks more than the cost of a ransom, a vulnerability that ransomware groups exploit. A ransomware threat assessment report found that customer financial data stolen during a ransomware attack was leaked 63 percent of the time, followed by patient data at 48 percent.[8]

Whether or not an entity pays the ransom, recovery is still expensive. In 2020, 560 healthcare facilities were hit with ransomware attacks in the United States, causing delays in patient care and costing victims millions of dollars in recovery.[9] Similarly, in 2019, the city of Baltimore refused to pay a ransomware demand that took its critical services offline, instead spending $18 million to rebuild and restore services.[10]

Federal agencies have maintained a stance against ransomware payments, instead urging impacted organizations to report attacks and share forensic evidence of potential intrusions on their network, otherwise known as indicators of compromise. The new Cyber Incident Reporting for Critical Infrastructure Act, once the Cybersecurity and Infrastructure Security Agency (CISA) completes the regulatory steps necessary, will require organizations to report certain cyber incidents to the CISA within 72 hours and ransomware payments within 24 hours.[11] Yet, the number of victims who report ransomware is likely a small proportion of the actual number of ransomware attacks.

3

# A Crisis Spurs Hard Questions

A ransomware attack can be a shocking, powerless moment for the victim. One incident response professional relayed his customer's experience this way: "One night, late at night, the guy's sitting there drinking his coffee, watching the widgets go down the production line, and things start to go wrong. Machines stop responding. Servers start doing strange things. Screens start popping up demanding [ransoms]."[12]

That feeling of confusion is common for victims of a ransomware attack. Norsk Hydro, a global aluminum and power company, described that moment of realization in a series of articles published after an attack on their systems in 2019:

> The bedside phone rang at 4 a.m. in Oslo, Norway. The pre-dawn call filled Torstein Gimnes Are with a drowsy sense of dread. That only deepened when he heard the first words from the other end. "We may be under attack," said his IT colleague . . . Production lines had stopped at some of its 170 plants. Other facilities were switching from computer to manual operations.[13]

Gimnes Are, the corporate information security officer, called the emergency preparedness chief. The next early morning phone call was to the new chief executive officer (CEO), as described in a *Time* article after the attack:

> [The CEO] answered the phone and heard what she assumed was a practical joke on the other end. . . . She said her colleague on the other end of the line told her: "We are under a severe cyber attack, you have to come to work. This is not a drill."[14]

The next set of decisions—and the level of disruption—for any company are determined by preparatory steps taken well before the attack. The following section is designed to, step by step, walk through

what would be a common experience for victims of a ransomware attack, based on a compilation of victim experiences, interviews with cybersecurity professionals, and published accounts. This section explores those questions for two hypothetical entities.

## The Attacks

### THE GLOBAL CORPORATION

Drive is a large, publicly traded car rental company. Malicious actors know that it is a partner of choice for the federal government and thus has global records of who rented cars and where and when they were rented. Given its large number of outposts worldwide and frequent interactions with customers through an app interface, it has a large potential attack surface.

In the early hours of a Saturday morning, Drive's rental office at the Frankfurt airport opens. Staff members turn on their computers and see blank blue screens. They cannot access any company systems, and a line of customers is beginning to form. Some customers are saying the app is not working either. The Frankfurt staff calls the help desk, only to hear it is a company-wide problem. The IT staff based in Pennsylvania is watching in horror as they are shut out of systems in a cascade of encryption.

A ransom note appears claiming attackers have compromised and encrypted systems, extracted millions of customer records, and compromised the app to steal information from customers' phones. Attackers are demanding $40 million for decryption keys, or they will sell sensitive company information to the highest bidder. The supervisor on duty calls the chief information security officer (CISO), who pauses momentarily before ringing the CEO at their vacation home in Idaho. It is 1:00 a.m.

Databases showing the locations of cars around the world are locked, preventing logging of rentals, returns, or emergency assistance to drivers. Drive has come to a global halt.

### THE SMALL UTILITY

VannWater is a small utility company that provides water to a handful of counties in Texas. It has served these communities for more than 50 years, and like many other utilities, it has connected its operational technology (OT) systems to the internet so that a small cadre of employees can monitor the health of the system from anywhere, minimizing the need for overnight staff at the facility.[15] However, they have not kept up with software updates, most of their OT systems are based on old technology, and they have yet to implement multifactor authentication for their employee access accounts.

It is 5:00 p.m. on a Friday in Texas, and the staff of VannWater is running final quality-control tests before heading home. As one operator opens the diagnostic system, the computer blinks to black. There are gasps of confusion as the other computers in the control room also blink and crash before a threat appears on the screen. The ransom note tells VannWater the attackers have control of water management systems and have extracted customer data from company networks. They are demanding $1 million in cryptocurrency in the next 12 hours.

Quality control systems are all down. For now, manual tests of water show normal chemical composition, but the employees are unable to make changes to the water management system.

Both entities are now faced with a set of questions including immediate response and long-term recovery.

## The Call

The heads of both entities have been informed of the attack. Who should the heads of the organizations call first?

- Legal representatives;
- The insurance company;
- An incident response firm; or
- Law enforcement.

Lawyers are almost always the first call. When some of Virginia Tech's servers were compromised as part of the Kaseya attack, the lawyers were the first non-IT staff called.[16] Ransomware attacks can mean huge liability for the victim entity, and mistakes made in the early chaos following an attack can have long-term consequences. Lawyers can also serve as an insulator for the firm: attorney-client privilege will protect some communications that could be used later in a lawsuit or investigation. Further, lawyers can serve as a liaison to protect the firm's interests with regulators, law enforcement, or shareholders.[17]

During the 2019 attack on Norsk Hydro, their emergency team met a few hours after receiving the ransom note. Executives made three swift decisions: they would not pay the ransom; they would summon Microsoft's cybersecurity team to help restore operations, and they would be fully transparent about the breach.[18]

Drive and VannWater, the two hypothetical entities, choose the following first steps:

- Drive's CEO calls in-house counsel, who gets dressed and goes to work. The lawyer has an updated, printed copy of the cyber incident response plan stored at the office. The legal representative has a silent moment of gratitude that Drive's cyberinsurance provider mandated that the company create a robust incident response plan and that the firm print a copy for their records.
- VannWater's president calls the outside counsel it has used before for property acquisition and personnel issues. That counsel is not a specialist in ransomware and instead recommends a colleague at a big firm in Houston. The Houston firm asks VannWater for a copy of their incident response plan and insurance policy information, but VannWater has neither.

## The Insurance Policy

VannWater did not buy cybersecurity insurance because premiums were too high, but Drive convinced their board to buy a policy at their last annual meeting. Drive's CEO had several levels of protection available to purchase:

- Comprehensive coverage, including additional legal counsel, incident response and forensics, any needed new hardware, and the services of a PR firm to help with public communications and client relations;
- Coverage for a ransomware payment up to $100,000 and services from an incident response firm; or
- Services from an incident response firm only.

As ransomware attacks have become more common and more expensive, insurance policies have emerged to fill the need for a safety net. Early policies demanded little of their customers by way of preparation or

defense. Insurance companies soon saw payouts on ransomware plans skyrocket, with extremely high loss ratios. The small but powerful group of reinsurers began to balk at backing these increasingly risky bets.

Naturally, the market responded. Premiums went up considerably—400 percent by one expert's estimate—and payouts declined drastically. One expert said that two years ago, a $40,000 premium would buy $10 million of coverage. Now, a premium twice as high will only buy half the coverage.[19] Further, insurance providers have begun to demand defensive measures to deem an entity insurable; without them, many entities discovered they were too high risk to cover when they attempted to renew their policies. However, this market adjustment has been incomplete. Cybersecurity policies, being new and different than traditional insurance, have been lightly regulated and thus vary widely. Not all insurance providers have the technical expertise to establish effective defensive measures or to adequately evaluate risk. As such, insurance plans are unevenly priced.

Interests inside entities are aligning between information security professionals and financial professionals as chief financial officers (CFOs) recognize the dramatic financial risk of lax security practices.[20] CISOs see insurers demanding security measures as a powerful ally for these internal discussions. As one expert said, "Boards pay the security budget when a cybersecurity insurance company comes and asks."[21] Another expert said that the insurance process will make an entity ask the right questions about cybersecurity practices, and "if you cannot pass that security check, then you definitely need cyber insurance!"[22]

Drive and VannWater made different decisions about insurance:

- Drive executives purchased the most comprehensive insurance plan they could find, which covered a suite of services. Their insurer, and its reinsurer, mandated as a condition of coverage that Drive create an incident response plan, engage in red teaming, and create automated, offline backups.
- VannWater considered insurance policies, but the rates had already skyrocketed, and affordable coverage provided very little assistance. The better insurance policies also would have required preventative steps that VannWater would not be able to implement quickly.

## The Status of Backups

Drive and VannWater evaluate offline backups to see what they can recover without paying the attackers to decrypt their files. After some investigation, these entities discover they have one of the following:

- Encrypted, offline backups from last week;
- Offline backups from four weeks ago; or
- Backups of critical data that were stored on-premises and were compromised in the attack.

Offline backups are critical to post-attack recovery. The National Institute of Standards and Technology (NIST) recommends preparing a "Go Bag" for data recovery, including passwords and security keys, kept in a secure location.[23] Various commercial solutions exist for automating backups, some aimed at OT systems and promising rapid, safe reboots. Even with offline backups, however, if the attacker has established a persistent presence in the system, older versions of company systems might also be infected. Virginia Tech's incident commander said, "We were fortunate that we knew when this happened . . . so we were able to go to the backups the day before that."[24]

Norsk Hydro eventually was able to restore some functionality from backups, but they were still offline for weeks and using paper systems to fill some orders.[25] *Time* recounted the return to long-

abandoned operating procedures: "Printed order forms, sticky notes on doors and black computer screens, hours of manual labor and extensive bookkeeping . . . Norsk Hydro relied on pen and paper to track its manufacturing and finances for about three weeks until computer access could be restored, only partially, and for mission-critical work."[26] That timeline was with the help of a global IT team and Norway's national cybersecurity organization.[27]

Drive and VannWater find the following when they attempt to pull their backup data:

- Drive backs up their most critical information to an offline database daily and keeps a year of backup data, so identifying a pre-breach copy and restarting their systems clean should be possible. However, the attackers have downloaded potentially embarrassing business emails, and the C-Suite is worried about information leaking out that might affect Drive's stock price. Further, government customers are worried about personally identifiable information being exposed, in particular movements of some undercover U.S. government officials.
- VannWater backs up its systems once a month. OT systems have not changed in that time span, but customer information may have changed. VannWater's one IT employee estimates it will still take weeks to verify the most recent backup is not tainted by the attack and to fully reset the OT system. VannWater calls in help from other utilities around the state to develop manual workarounds for water testing and adjusting levels of chemicals.

## The First Responders: Forensics and Incident Response

Both Drive and VannWater also seek to quickly figure out what systems are compromised and where malware might lurk in their network, along with engaging in forensic research to find out how the breach occurred. Neither company is confident they can do this alone. Should they hire an incident response firm?

- Yes, Decide to hire a firm; or
- No, Decide not to hire a firm.

Most companies do not have a robust security team qualified to respond to a ransomware breach. The Information Systems Audit and Control Association's *State of Cybersecurity 2021* report found that 55 percent of respondents cannot fill all of their open cybersecurity positions.[28] Incident response firms can be an important guide for such organizations as they juggle several priorities, such as recovering data, informing customers, and navigating legal requirements. These firms can facilitate the investigation process and may also be reassuring to customers. Working with an experienced cybersecurity firm can save precious time and make the cleanup process smoother.

Kaseya, for instance, immediately retained cyber security firms during its massive breach, a move that proved valuable in containing the attack, preventing further spread, and reassuring clients.[29] By engaging its internal response team with external cyber forensics experts, Kaseya was able to drill down to the root cause of the attack and assess its larger impact. Incident response firms are also helpful in identifying indicators of compromise (IOCs) to isolate accessed systems and data.

IT and security teams face a lot of pressure from executive teams to bring systems back online, making it more challenging to respond to and contain an attack. While assisting during a ransomware attack, incident response teams prioritize investigation and analysis of the malware and infected servers, provide guidance in developing a recovery timeline, identify documentation requirements, and assist in communications if needed.

Both hypothetical entities decide recovery is beyond them and immediately seek to hire the best incident response team they can afford.

- Drive uses some of its insurance payout to hire an incident response firm who can assist with forensics and recovery. Drive hires a separate crisis management PR firm to handle communications strategy.
- VannWater has limited funds, but an up-and-coming, Texas-based cybersecurity firm offers to help for a reduced price. They offer forensic services and to coordinate with the Federal Bureau of Investigation (FBI) and CISA.

## The Communication Strategy

Customers of both entities figured out something was wrong almost right away. They are now getting more insistent. Tweets are becoming increasingly pointed and alarmist; media outlets have called to ask if there is a cybersecurity breach. The companies are still at the early stages of the investigation, however, and do not yet know the scope of the problem or the extent of the damage. What do they say to their customers and the public?

- Delay engagement—there is not enough information yet;
- Pursue full transparency—better to release what is known than to feed rumors with silence; or
- Report there has been a cyber incident, but nothing more.

Emergency response teams have limited information and intense time pressure, including from anxious or stranded customers, but entities must still make carefully considered decisions about communications. There is a very human desire to reassure and to "fix it" as soon as possible. Entities eager to say something quickly can forget key elements, such as ensuring legal review of any statements.

Entities factor in a number of elements when deciding how to communicate during the immediate aftermath of an attack, from regulatory requirements to company culture. Norsk Hydro, for example, chose radical transparency, for which they received accolades.[30] Webcasts, daily press conferences, a social media push, and extensive access for journalists were key elements of their communications strategy, in addition to creating a new company website designed specifically to answer questions about the attack.[31] Despite the loss of tens of millions of dollars, the company's stock price proved resilient, likely in part to their aggressive communications strategy. Plus, their open data sharing with the government of Norway almost certainly protected other entities from the same fate.[32]

Companies also must decide who carries out the communications. CEO engagement may be necessary with some high-profile stakeholders, but executives cannot be everywhere. Account managers are the most likely interlocutors for customers, but they necessarily will have limited information, in part due to the complication of secure communications. Email is out of the question because it might tip off the attackers to countermeasures and plans, which leaves text chains and phone calls. A well-meaning but underinformed account executive could accidentally spread bad information and cause confusion.

Still, those who navigate these challenges adeptly have an opportunity to enhance their reputation. Ransomware attacks are so common that entities are judged far more on their response to an attack than the fact that an attack occurred. One expert pointed out the potentially dire consequences of getting things wrong: "You could turn an opportunity for credibility into one that damages your credibility."[33]

Drive and VannWater choose the following for their communication strategies:

- Drive decides to issue a statement early on that they have suffered a ransomware attack and that their first priority is to keep customers on the road. They make no statements yet on the extent of the damage or how long they expect systems to be down, but they reassure customers that a competitor will honor existing reservations for the next week.
- VannWater's customers depend on them for water, and they are demanding answers on whether the drinking water is safe. Independent testing suggests the water quality has not changed, but real-time monitoring is down. VannWater issues an immediate statement that customers should drink bottled water and holds a press conference alongside local government officials to discuss potable water distribution on an emergency basis. They also describe their plan for manual testing and operation of the water system, and while they do not promise a date for a return to service, they say they will test the manual system for a full 24 hours before advising customers the water is safe.

***Ransomware attacks are so common that entities are judged far more on their response to an attack than the fact that an attack occurred. One expert pointed out the potentially dire consequences of getting things wrong: "You could turn an opportunity for credibility into one that damages your credibility."***

## The Long Recovery

Both companies want to start recovery right away, but incident response firms warn that attempting to restart systems before the attackers' footholds have been verifiably eliminated is risky. Backups could be compromised, and the companies could be reinfected. What is the next step?

- Restart immediately with the most recent backup that is assumed to be safe;
- Partial restart—turn on systems that appear unaffected and can be segregated from the compromised machines; or
- Wait for a full evaluation before restarting anything.

A company's first instinct is to get back up and running immediately, but that can be a risky choice. There is a balance between minimizing downtime while also reducing risk that the attackers are still lurking, ready to reinfect backups. One incident response provider said the work to fully oust the attackers from the systems requires focus and commitment.[34]

Still, incident response experts say that recovery can start a lot earlier than customers expect but take much longer than might be anticipated.[35] Supervisory control and data acquisition systems often run on old hardware, firmware, and software that have to be completely rebuilt. One expert said that businesses tend to move quickly to recover customer data or customer-facing systems because of

regulatory requirements or reputational concerns but are more likely to be cautious with systems that govern internal operations. For customer systems, the goal is to return to operations in two hours. For internal attacks, executives may be uncertain about how to recover and, faced with operational challenges, delay making decisions.[36] One expert estimated that remediation for the average large enterprise takes 80 days, with the initial "sprint mode" lasting about three weeks.[37]

Drive and VannWater find themselves under different pressures:

- Drive uses recent backups to reopen their records of upcoming car rentals. They send that data to a competitor who has agreed to honor car reservations for the next week. Drive's first priority is to restore their internal tracking and billing systems and track their inventory of cars; meanwhile they instruct their field offices to keep records using a hastily constructed paper system.
- VannWater follows the advice of their incident response firm and chooses to restart as soon as possible, despite some risk. There cannot be a halt in water flows during a hot Texas summer.

## The Federal Authorities

Forensics teams have recovered some indicators of compromise and established how the attackers have moved across the systems. They still are not sure how the attackers got in, but they suspect an employee opened a phishing email. Should the companies call government authorities?

- Do not alert the government—it could mean investigations and liability, with no clear upside;
- Call the local FBI field office;
- Reach out to CISA; or
- Call local law enforcement.

When Virginia Tech was working through the implications of the Kaseya ransomware attack, they contacted Virginia Tech's campus police force and the FBI office in Richmond. According to Jeffry Lang, who ran the incident response, the FBI didn't have a lot of information. The Richmond FBI field office did pass on additional information from a different field office running point on that investigation. Virginia Tech also opened a case with the Internet Crime Complaint Center.[38]

Many victims describe their interactions with the FBI as a one-way street, where the entity provides information about the attack and gets nothing in return.[39] From the entity's perspective, they are exposing themselves to risk by sharing. Some insurance companies have a requirement that the entity call the FBI when they file a claim.[40] Many incident response firms have longstanding relationships with the FBI, CISA, and the National Security Agency and can capably provide IOCs stripped of any confidential information. The FBI has helped some victims by providing guidance based on similar attacks they have seen and the attackers' tactics, technologies, and procedures (TTPs). In rare cases, they can assist with a universal decryption key.[41]

Drive and VannWater choose engagement with the government:

- Drive's insurance policy requires that they reach out to the FBI with IOCs, so Drive asks their incident response firm to facilitate that interaction, with the help of legal counsel. The FBI is concerned about the counterintelligence implications of the information the attackers might have gleaned on the movement of U.S. government officials overseas. They tell Drive they are tentatively attributing the attack to a Russian hacking group loosely affiliated with the Russian

government, based on the TTPs, which was also the conclusion of the incident response firm. They do not have a decryption key for this attack.

- VannWater calls CISA, drawing on the connections they have established through their Information Sharing and Analysis Center (ISAC) and other critical infrastructure groups. CISA is grateful for the shared information and IOCs and offers up their ransomware recovery guide and technical assistance.[42] They also recommend that VannWater reach out to the FBI. They do not have a decryption key for this attack.

## To Pay or Not to Pay

The attackers are demanding payment within 24 hours and threatening a release of embarrassing information. They seem to know that the companies have reached out to the FBI and CISA and are claiming that they will raise their ransom demand if the federal government attempts to assist. They are currently demanding $500,000 from VannWater and $4 million from Drive. Should the companies pay?

- Yes—systems need to be running immediately and the companies are willing to pay to get at least some functionality back;
- No—the companies do not want to reward this criminal behavior and think they can recover enough systems from backups; or
- Negotiate—the ransom demands are too high to be cost-effective, but paying a lower amount might be worth it.

Once an entity makes contact with the attackers, the clock starts. Attackers want to bully victims into quick payment. But to negotiate effectively, an entity needs to know what the attackers have, where they are on the systems, and what they stand to lose if the data stays encrypted or if confidential material is publicly released. Michael Rogers recommended, in a presentation at the 2022 SANS Ransomware Summit, that entities not begin negotiations until initial forensics are complete and counsel provides exposure estimates.[43]

Entities are faced with an extremely difficult choice when considering paying a ransom. Paying is expensive and marks the company as a profitable target for criminals. On the other hand, a natural instinct is to pay and get the crisis over with quickly, but that hope rarely materializes. One expert said customers assume payment leads to keys that immediately unlock data, when in reality keys only sometimes work, and the process of installing them is onerous and slow—often requiring manual installation, computer by computer, with days needed to run decryption.[44]

Virginia Tech debated paying the ransom during the Kaseya attack. The attackers demanded $44,000 per key, and the university would have needed an estimated 1,000 keys to unencrypt everything—a prohibitively high cost. University staff decided their highest priorities were about 30 machines, and they offered the attackers $700,000 to decrypt those.[45] In the end, they did not pay the ransom because they were able to recover some data on their own.

Another victim, Sonoma Valley Hospital, found its continuity plan was sufficient to maintain operations by bypassing the impacted servers and using information stored on offsite backups.[46] They did not pay the ransom.[47] A separate entity had run the numbers and was ready to pay, but midway through the negotiation the attackers raised the price. The cost-benefit analysis no longer made sense, and the company chose to recover what they could on their own.[48]

***Entities are faced with an extremely difficult choice when considering paying a ransom. Paying is expensive and marks the company as a profitable target for criminals. On the other hand, a natural instinct is to pay and get the crisis over with quickly, but that hope rarely materializes.***

Norsk Hydro decided it would not pay the ransom. One senior vice president who was on the response team said, "I think our decision was confirmed later on because once your system is encrypted, a lot of damage has already happened along the way . . . even if you get the encryption key [from the attackers], there's no guarantee it will work, and you still have to fix the problem that your system has been compromised." Rebuilding essential systems took about three weeks; rebuilding and restarting the user directory, cloud services, and other systems took about three months.[49]

Ann Johnson, Microsoft's corporate vice president of cybersecurity solutions who helped oversee the Norsk Hydro recovery, says that companies tend to be tempted to pay to regain their data, but that payment provides no guarantees of recovery.[50]

After consultation with legal counsel and the FBI, Drive and VannWater decide the following:

- Drive runs the numbers on the cost of recovery and decides not to pay. Drive's backup data is good enough to get started on full recovery. The C-Suite is still worried about the reputational cost of leaked emails, but after an internal damage assessment, they have decided it is worth the risk.
- VannWater decides to negotiate and brings the ransom demand down to $250,000, paid in cryptocurrency. They have already laid the groundwork with the FBI to try to recover some or all of those funds after decryption keys have been delivered. In the final accounting, The FBI was able to recover more than half of the funds. However, decryption keys were only partially successful in restoring operations.

## Final Results

The two hypothetical companies took different paths to deal with their ransomware attacks, reflecting very different resourcing pictures. Drive spent time and money building in resilience before an attack, including buying insurance, creating secure offline backups, and writing a playbook. As a result, they had a plan during the attack and available resources to get assistance. VannWater had made no such preparations. They had a more chaotic, riskier road to recovery, with haphazard crisis decisionmaking. Still, both companies experienced significant disruptions, with Drive's customers at least temporarily stranded, and VannWater's Texas customers living without a dependable water supply. VannWater's experience is meant to represent the situation of many public utilities—low on resources but long on responsibility to the public. Disruptions to utilities can be a life and death situation.

# Two Paths through a Ransomware Attack

PATH ONE (P1)

## Comprehensive Preparation

Your entity chose to do all of the following things in preparation for a potential attack:

- ✓ Buy insurance
- ✓ Develop a relationship with the FBI Field Office
- ✓ Backup systems and data frequently
- ✓ Store those backups offline
- ✓ Create a ransomware attack playbook
- ✓ Exercise that playbook

PATH TWO (P2)

## Deferred Preparation

You and your leadership team did not think your organization would be a target for attackers. You delayed taking the following precautions:

- ✗ Buy insurance
- ✗ Develop a relationship with the FBI Field Office
- ✗ Backup systems and data frequently
- ✗ Store those backups offline
- ✗ Create a ransomware attack playbook
- ✗ Exercise that playbook

**When the attack happens, you have the following choices to make:**

### WHO DO YOU CALL FIRST?

| P1 | P2 |
|---|---|
| ○ Insurance | ○ Insurance |
| ○ Lawyers | ○ Lawyers |

### WHAT IS THE STATUS OF YOUR BACKUPS?

| P1 | P2 |
|---|---|
| ○ Available | ○ Available |
| ○ Compromised | ○ Compromised |
| | ○ What backups? |

### WHAT DO YOU BUY WITH YOUR INSURANCE?

| P1 | P2 |
|---|---|
| ○ Incident Response Firm | ○ Incident Response Firm |
| ○ Replacement Hardware | ○ Replacement Hardware |
| ○ PR Consultants | ○ PR Consultants |
| | ○ No Insurance |

### WHEN DO YOU ISSUE A STATEMENT?

| P1 | P2 |
|---|---|
| ○ Immediately (despite incomplete information) | ○ Immediately (despite incomplete information) |
| ○ When regulatory authority requires | ○ When regulatory authority requires |
| ○ Only when the incident is over | ○ Only when the incident is over |

### WHEN DO YOU TRY TO RECOVER FUNTIONALITY?

| P1 | P2 |
|---|---|
| ○ The sooner the better, despite the risk | ○ The sooner the better, despite the risk |
| ○ When the incident response team recommends | ○ When the incident response team recommends |
| ○ Not until we are sure all adversary presence is gone | ○ Not until we are sure all adversary presence is gone |

### DO YOU CALL THE GOVERNMENT?

| P1 | P2 |
|---|---|
| ○ Yes – the FBI Field Office | ○ Yes – the FBI Field Office |
| ○ Yes – the CISA hotline | ○ Yes – the CISA hotline |
| ○ No – why? I expect to get nothing in return | ○ No – why? I expect to get nothing in return |

### DO YOU PAY THE RANSOM?

| P1 | P2 |
|---|---|
| ○ Yes – it's worth it to avoid embarrassment and continued losses | ○ Yes – it's worth it to avoid embarrassment and continued losses |
| ○ No –although our insurance will pay for it, we will try to recover by ourselves | ○ No – we can't afford it; we will try to recover by ourselves |
| ○ No – It's morally wrong and probably won't work anyway | ○ No – It's morally wrong and probably won't work anyway |

*Entities that choose to comprehensively prepare have far more options available to them in the event of a ransomware attack. Entities that choose preparation—the path on the left—can move through the "P1" set of options below. Entities that do not prepare—the path on the right—are stuck in the far more restricted "P2" set of options. The choices in gray are not available to the less prepared entities.*

Source: Based on authors' original analysis.

4

# Findings

## Preparation Makes the Difference

The most important phase of a ransomware attack is before the attack happens. With ransomware attacks widespread, entities should assume an attack is coming and should prepare as if it will happen next week. These preparations fall into two buckets: common-sense defense and contingency planning. Basic steps such as multifactor authentication and creating offline, secure backups can mean the difference between disaster and resiliency in the face of a ransomware attack. Adopting a zero-trust approach can prevent an initial penetration of a system from turning into a catastrophe.[51] As the Institute for Security and Technology's Ransomware Task Force found, "Although any organization, regardless of its security, can be a target for a ransomware attack, improving baseline security and raising awareness among employees can go far in protecting organizations from attack."[52]

Contingency planning is the second half of preparation. Companies that created a playbook, wrote it down in detail, and exercised the playbook were also much better prepared to react quickly and effectively in the early stages of an attack. All three companies that the Senate Homeland Security and Government Affairs Committee (HSGAC) interviewed for its ransomware report had established incident response plans that "allowed each entity to take quick remedial action, onboard third-party experts, and in the case of Entity B cut off the attacker's access before they encrypted its networks with ransomware."[53] Interviewees said that the difference between victims who have worked through a playbook and those who have not is stark, with the latter operating in a state of heightened confusion and chaos.

## Insurance Markets Are Becoming More Sophisticated

The market forces surrounding cyber insurance are slowly lowering payouts and enhancing customers' cyber defense, likely making the insurance market a net positive for cybersecurity practices. Insurance providers are getting more savvy about the risks, and policy holders increasingly need to prove they engage in good cyber hygiene in order to qualify for a policy. However, progress has been uneven, as some insurance providers have not yet developed the necessary expertise to judge how risky a policy might be.

## Court Rulings on the War Exclusion Could Be a Wildcard

A potential wildcard in the insurance markets, however, is the problem of the war exclusion. Many insurance policies include language like: "This insurance does not apply to loss or damage caused directly or indirectly by war, invasion, act of foreign enemy, hostilities (whether war be declared or not) . . . or military power." Attribution of a ransomware attack then becomes a critical financial issue. There is an ongoing debate about the extent to which some nation-state actors support ransomware attacks or have a de facto policy of benign neglect. Russia in particular has a reputation for allowing criminal groups to operate in their territory, provided those groups only harass Western entities and do occasional favors for the Russian government.[54]

Courts are beginning to hear cases about when the war exclusion becomes relevant. In a recent case about losses Merck incurred because of the NotPetya attack, a New Jersey court found that the war exclusion did not apply, but the ruling was narrow. The court decided that the insurer in question had the opportunity to put policyholders on notice that the exclusion would apply to cyberattacks rather than just "traditional" forms of warfare, but they failed to do so.[55] Lawyers for the insurer were quick to object: "The decision relies upon case law rendered before the internet existed and before 'cyber' was a word. The reasoning of this decision looks backward to a century past, and we believe it will not age well."[56] Lloyds of London earlier this year tweaked its definitions to partially address this problem.[57]

The most clear-cut example of cyber activity surrounding a conflict involves the Russian government attacking Ukraine's power grid in conjunction with their invasion this year, but other recent examples are more complicated: does the 2015 attack on Ukraine's grid count as "war?" What about pro-Russian hackers attacking the United States or Norway because of Washington and Oslo's support for Kyiv?[58] What are the implications of the 2019 ruling of the Ninth Circuit Court of Appeals that the war exclusion only applies to "hostilities between de jure or de facto governments?"[59] What if the attackers are a criminal gang, but there is evidence some members of that gang are working at the behest of a government's intelligence service? In this context, an offhand remark by a national security official that a ransomware attack was sanctioned by a nation-state could be evidence in an insurance case with billion-dollar implications. Some rocky legal battles are ahead, and the precedent they set will have wide-ranging impacts.

*An offhand remark by a national security official that a ransomware attack was sanctioned by a nation-state could be evidence in an insurance case with billion-dollar implications.*

## Law Enforcement Is Minimally Helpful during an Attack but Vital for Collective Defense

The general consensus among interviewees and in available reports from victims is that calls to the FBI rarely result in tangible benefits during a crisis. One victim told HSGAC that "Entity A found the FBI to be unhelpful throughout the process," including because "Entity A asked [the] FBI for best practices and other guidance documents but did not receive helpful assistance." Two other case-study victims found the FBI minimally helpful.[60]

The FBI's main role is to build evidence for legal action against accused criminals, not provide assistance in recovery from criminal behavior. One entity told HSGAC that the "FBI prioritized investigating those responsible for the attack over helping Entity A respond and secure its network—the top priority for Entity A."[61] These mismatched priorities are frustrating for both sides but understandable. The FBI is not resourced for providing assistance.

*The general consensus among interviewees and in available reports from victims is that calls to the FBI rarely result in tangible benefits during a crisis.*

However, the FBI can be a critical central point for collective defense. Passing indicators of compromise on to federal authorities protects other entities from those same attackers. The FBI sometimes will have universal decryption keys or insights into attacker tactics, technologies, and procedures that can assist in ousting attackers from compromised systems. Sharing data with the FBI is beneficial for future safeguarding of other companies against similar attacks.

5

# Recommendations

## Recommendations for Policymakers

### DISINCENTIVIZE RANSOM PAYMENTS, REPORT ATTACKS, AND SUPPORT VICTIMS

It is understandable for victims to hope to minimize damage by paying a ransom. One expert put it bluntly: "Banning payments seems anti-victim. Should they pay the ransom or lay off half their people? It's a stark choice for some."[62] But those payments fuel additional attacks, in essence funding a cycle that leads to more victims. Thanks to high insurance premiums, low ceilings for ransom payment reimbursement, and flawed decryption keys, the market is slowly shaping incentives to improve security practices and focus on self-recovery rather than paying ransoms. These market forces will likely push the supply and demand curves to a point where successful attacks and payments are less frequent, but those trends do not suggest a rapid end to the phenomenon of ransomware.

Recently enacted legislation will use regulatory authorities to require critical infrastructure owners and operators to report cyber incidents and ransomware payments to CISA.[63] Policymakers should implement this law, evaluate its success at the one-year mark, and then adjust the legislation to fix any revealed flaws. They should then expand this requirement to all victim entities. This data collection will enhance accountability for those paying and help the U.S. government collect information about the scope of the problem, identifying trends and patterns.

Policymakers need to further disincentivize ransom payments. Congress should consider instituting a penalty of 10 percent of the ransom, phased in over several years to give companies time to adjust. The revenue from any such penalty should go to fund CISA's cybersecurity education and support programs.

Policymakers should also consider creating a government-sponsored safety net for small businesses, nonprofits, public utilities, schools, and local government entities that suffer a catastrophic attack. Entities who pay the ransom would be ineligible for help. This effort would need to avoid creating a moral hazard, still encouraging advances in cyber hygiene. For example, CISA could run a program where entities register for the safety net and then receive a CISA vulnerabilities scan and a cyber hygiene checklist. When they have completed the steps required by the checklist, such as creating offline backups of critical systems, implementing multifactor authentication, and agreeing to share any indicators of compromise (IOCs) with the FBI and CISA, they can buy into a limited assistance program. That program might provide something like 50 percent of payroll for two weeks to give entities breathing space to recover from an attack.

### INCREASE SOCIAL PRESSURE FOR CYBER HYGIENE

Recognizing the centrality of cybersecurity to good business practices, organizations such as the Better Business Bureau and industry associations should publicly praise businesses that improve their cyber practices. That pressure could speed a cultural shift toward collective defense, where entities recognize the harm they cause others by paying ransoms and the support they have for improving security practices. In one example of increased scrutiny, Moody's has started evaluating cyber risk as part of their larger risk evaluation program.[64]

It is also worth exploring creating tax credits for cybersecurity efforts. The U.S. government has used the tax code to shape behavior, such as tax credits for green upgrades. Hybrid car tax credits, solar tax credits, and energy efficient appliances, and windows credits all make such steps slightly more affordable and create incentives. Certifying actual progress in cyber hygiene would be challenging, but the difficulties and potential fraud are worthwhile risks in order to prompt progress.

### TAX CREDITS FOR INFORMATION SHARING

Similarly, tax credits for sharing detailed information about a ransomware attack could incentivize companies to pass more information on to the FBI or CISA. Attempting to judge the quality or quantity of information would be complicated and controversial, but the "fact of" reporting a compromise and associated details to the FBI or CISA could generate a receipt for tax purposes, much like a charitable donation.

### BROADEN INFORMATION SHARING AND ISAC COLLABORATION

As ransomware threat actors use similar TTPs to target multiple organizations, threat intelligence sharing must be further broadened across industry sectors. If one organization detects a ransomware attack early, it can proactively alert other organizations through sharing of attack vectors to prevent spread. This sharing should be fully automated—it is asking for extreme altruism for a targeted organization to pause mitigation efforts to share IOCs.[65]

ISACs are important venues for safe information sharing among companies from the same sector, but effective information sharing requires sustained investment of time, people, and money.[66] Entities should invest in these organizations, and ISACs should increase sharing on changes in the threat picture and help companies implement best practices.[67] Further, ISACs should abandon silos and facilitate sharing IOCs across sectors. Victims of ransomware and other cyberattacks are not restricted to one sector; instead, there should be robust sharing between ISACs.[68] On a tactical level, ISACs should improve sharing on non-technical items like samples of phishing emails. Finally, CISA should

work with ISACs to automate as much of the process as is feasible, from submission to processing to sharing to intake. Ideally, collaboration should happen in real time.[69]

### MANAGE EXPECTATIONS AND TREAT VICTIMS AS PARTNERS

The U.S. government needs to better communicate the extent of help it can provide to victims and the circumstances in which assistance can be provided. It should clearly state during interactions with victims that the FBI investigates while CISA can provide limited assistance. The FBI and DOJ have committed to more aggressive action on ransomware, pledging to open cases quicker and to raise the number of seizures or forfeitures by 10 percent.[70] Realistically, the FBI itself is too resource constrained to investigate every ransomware attack, and they should manage victim expectations about the FBI's capacity for follow up. Despite these constraints, The FBI also needs to understand the victim's perspective and think about growing the partnership with interactions rather than just being in receive mode for information about an attack.

### ADVERTISE EXISTING FRAMEWORKS FOR SECURITY STANDARDS

Entities look to credible, independent bodies for direction on what good cybersecurity looks like. NIST created a cybersecurity framework in 2014, and the Institute for Security and Technology has identified the top controls that defend against ransomware. CISA, FBI, and ONCD should use their positions to advertise these standards to business, state and local governments, and insurance groups.[71] Insurance companies can underwrite to that standard and entities will work to comply.[72]

## Recommendations for Industry

### ADOPT A SECURITY MINDSET

Making the time to exercise a crisis and investing in cybersecurity can seem like a waste to a business if there is no clear and present threat. But data suggests a ransomware attack is not just possible but likely, and the threat is constantly shifting. As one interviewee said, "Someone could plug in a new toaster, and everything could change."[73] A proactive approach to basic security steps is far more cost-effective than hemorrhaging cash in a crisis.[74] The C-suite and its equivalent in smaller organizations must set aside time—even an hour at a strategy offsite—to evaluate their own risk picture and make a plan for response.

### MAKE A PLAYBOOK

An entity can take all the available defensive measures and still suffer a ransomware attack. All entities should have a playbook for response in the first hours, days, and weeks. That playbook should at a minimum have the following:

- A prioritized asset list: Entities should know what equipment touches their network, where sensitive data is stored, and what systems are most critical to a rapid recovery. Entities should also determine which systems are most critical to operations and how long those systems can be offline before operations suffer significant impacts. For critical infrastructure owners and operators, organizations should go a step further to determine how long systems can be offline before there are regional or national effects.[75]
- The right team: Entities must know—and rehearse—how teams can make quick decisions and who can serve as a backup point of contact when needed. If the CEO is unavailable, who can

make a decision in their place? Further, who is on the response team? In a medium-sized business it can include the executive team, the technical team, counsel, security operations, negotiators, forensics and incident response, and cyber insurance. There might be 25 people engaged, more than 16 of those from outside of the organization.[76]

- Insurance documents: If an entity has insurance, there should be an offline version of the insurance policy, preferably included in the playbook.[77] Online copies should not include information on ransomware payment support, lest the attackers find out how large a payment insurance will cover.
- Details on how to reach local and federal government officials: The FBI, CISA, and U.S. Secret Service should be on the call list, along with state-level emergency or incident response centers, if available.[78]

## KNOW YOUR GOVERNMENT CONTACTS

While incident response plans should include details about how to reach government contacts, a crisis is the wrong time for that first phone call. The FBI, CISA, and Secret Service all have resources on preparing for a cyber incident and have made public pledges in recent years to engage with entities across the spectrum.[79]

## MAKE A COMMUNICATION STRATEGY

Entities should decide up front whether the default policy will be transparency or whether some degree of confidentiality is a better approach. When exercising a playbook, communications with the public, shareholders, and any regulatory or other oversight bodies should be factored in. Norsk Hydro's executives believed their decision in the early hours to be completely transparent about their ransomware attack resulted in minimal damage to their reputation and share price. One Norsk senior vice president said, "Actually on that day, our share price over-performed the market, which is, in theory, hard to imagine when you tell [sic] that you have been victim of Norway's largest cyberattack."[80]

6

# Conclusion

Ann Johnson, corporate vice president of security, compliance, and identity business development at Microsoft, summed up the importance of preparing for an attack: "Your data is a strategic asset for you, and for cybercriminals. That's why they want it. It is also why your data must be protected . . . the best defense is to ensure you have the right combination of people, processes, and technology."[81]

This study builds on the excellent work of the Institute for Security and Technology's Ransomware Task Force and the Senate Homeland Security and Government Affairs Committee to encourage a stronger understanding of the business perspective. Most of the recommended measures for industry and government are neither new nor novel. They are not difficult to understand, just sometimes difficult to implement. Entities that use the time and resources to work through a response playbook, carefully evaluate the risks to the business alongside the cost of preparatory steps, and implement simple defensive measures will save confusion and damage in the event of an attack, but this requires preparation well before the attack. Policymakers know ransomware is a scourge, but they need to understand that entities face difficult, sometimes existential decisions. Policy needs to shape incentives gently toward information sharing and away from paying ransoms.

# About the Authors

**Emily Harding** is deputy director and senior fellow with the International Security Program at the Center for Strategic and International Studies (CSIS). She joined CSIS from the Senate Select Committee on Intelligence (SSCI), where she was deputy staff director. In her nearly 20 years of government service, she has served in a series of high-profile national security positions at critical moments. While working for SSCI, she led the Committee's multiyear investigation into Russian interference in the 2016 elections, which resulted in a five-volume, 1,300-page report. During her tenure on the Committee, she oversaw the activities of 18 intelligence agencies and led SSCI staff in drafting legislation, conducting oversight of the intelligence community, and developing their expertise in intelligence community matters. She began her career as a leadership analyst at CIA, and then became a manager of analysts and analytic programs. She led the Iraq Group during the attempted Islamic State takeover of Iraq and Syria and led a multidisciplinary group of analysts working crises worldwide. During a tour at the National Security Council, she served as executive assistant to the deputy national security adviser for global democracy strategy and then as director for Iran, where she led interagency efforts to create innovative policies drawing on all elements of national power. After leaving the White House, she served on a team running the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for liaising with both campaigns and briefing the incoming administration on a wide range of intelligence topics. Harding holds a master's degree in public policy from Harvard University's Kennedy School of Government and a bachelor's degree in foreign affairs from the University of Virginia.

**Harshana Ghoorhoo** is a research assistant with the CSIS International Security Program, where she conducts research in cybersecurity, artificial intelligence advancement, and the intersection of emerging technologies and national security. Prior to joining CSIS, she interned with the Modern

War Institute at West Point Academy, where she researched urban warfare as well as military strategy during the Revolutionary War. She holds bachelor's degrees in international relations and philosophy and modern languages from Seton Hall University.

# Endnotes

1 See "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," The White House, October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/; "Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

2 "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing over $30 Million in Losses," U.S. Department of Justice, November 28, 2018, https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

3 "Alleged Russian Cryptocurrency Money Launderer Extradited from the Netherlands to the United States," U.S. Department of Justice, August 17, 2022, https://www.justice.gov/usao-or/pr/alleged-russian-cryptocurrency-money-launderer-extradited-netherlands-united-states.

4 "80% of Critical Infrastructure Organizations Experienced Ransomware Attacks Last Year," Claroty, February 3, 2022, https://claroty.com/press-releases/80-of-critical-infrastructure-organizations-experienced-ransomware-attacks-last-year. Claroty also reported: "Of the 80% of respondents who experienced a ransomware attack, 47% reported an impact to their industrial control system (ICS) environment and over 60% paid the ransom, more than half of which cost $500,000 or more. Additionally, the majority of respondents estimated a loss in revenue per hour of downtime to their operations equal to or greater than the payout. Even among those who did pay the ransom, 28% still experienced substantial impact to operations for more than a week."

5 Ibid.

6 Rachel Monroe, "How to negotiate with ransomware attackers," *The New Yorker*, May 31, 2021, https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.

7 IBM Security, *Cost of a Data Breach 2021* (Armonk, NY: IBM, 2021).

8 Rapid7, *Pain Points*: *Ransomware Data Disclosure Trends* (Boston, MA: Rapid7, 2022), https://information.rapid7.com/rs/411-NAK-970/images/Ransomware%20Data%20Disclosure%20Report.pdf.

9 Ransomware Task Force, *Combatting Ransomware*, *A Comprehensive Framework for Action: Key recommendations from the Ransomware Task Force* (San Francisco, CA: Institute for Security and Technology, April 2021), https://securityandtechnology.org/ransomwaretaskforce/report/.

10 Ibid.

11 "President Biden signs into law the cyber incident reporting for critical infrastructure act, expanding cyber reporting obligations for a wide range of public and private entities," Gibson Dunn, March 22, 2022, https://www.gibsondunn.com/wp-content/uploads/2022/03/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities.pdf.

12 Carl Eshelman, "The Anatomy of a Targeted Industrial Ransomware Attack," YouTube video, posted by SANS Institute, July 20, 2022, 24:33, https://www.youtube.com/watch?v=kNTw8pbq2EY&ab_channel=SANSInstitute.

13 Bill Briggs, "Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency, Microsoft/Transform, December 16, 2019, https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/.

14 Patrick Lucas Austin, "This Company Was Hit with a Devastating Ransomware Attack—But Instead of Giving In, It Rebuilt Everything," *Time*, July 14, 2021, https://time.com/6080293/norsk-hydro-ransomware-attack/.

15 Warwick Ashford, "Norsk Hydro Confirms Ransomware Attack," ComputerWeekly.com, March 19, 2019, https://www.computerweekly.com/news/252459707/Norsk-Hydro-confirms-ransomware-attack.

16 Jeffry Lang, "Kaseya Ransomware Reaction—Lessons Learned," YouTube video, posted by SANS Institute, August 11, 2022, 31:14, https://www.youtube.com/watch?v=5cMsmB4PlbM.

17 Committee on Homeland Security and Governmental Affairs (HSGAC), *America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies* (Washington, DC: U.S. Senate, March 2022), 42, https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf.

18 Briggs, "Hackers Hit Norsk Hydro."

19 Interview with Expert 1.

20 Ibid.

21 Ibid.

22 Interview with Expert 3.

23 "Protecting Data from Ransomware and Other Data Loss Events," National Cybersecurity Center of Excellence, NIST, April 2020, https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf.

24 Lang, "Kaseya Ransomware Reaction."

25 Ashford, "Norsk Hydro Confirms Ransomware Attack"; John Evans, "The Norsk Hydro Attack," Industrial Cyber, March 24, 2019, https://industrialcyber.co/features/the-norsk-hydro-attack/. Austin, "This Company Was Hit with a Devastating Ransomware Attack."

26 Austin, "This Company Was Hit with a Devastating Ransomware Attack."

27 Ashford, "Norsk Hydro Confirms Ransomware Attack."

28 "State of the Cybersecurity Workforce: New ISACA Research Shows Highest Retention Difficulties in Years," Information Systems Audit and Control Association (ISACA), March 23, 2022, https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new-isaca-research-shows-retention-difficulties-in-years.

29 "Updates regarding VSA security incident," Kaseya, July 2–26, 2021, https://www.kaseya.com/potential-attack-on-kaseya-vsa/.

30 Austin, "This Company Was Hit with a Devastating Ransomware Attack."

31 Briggs, "Hackers Hit Norsk Hydro."

32 Austin, "This Company Was Hit with a Devastating Ransomware Attack."

33 Interview with Expert 3.

34 Eshelman, "The Anatomy of a Targeted Industrial Ransomware Attack."

35 Rogers, "Ransomware Management and Recovery Tactics."

36 Interview with Expert 2.

37 Rogers, "Ransomware Management and Recovery Tactics."

38 Lang, "Kaseya Ransomware Reaction."

39 Interview with Expert 1.

40 Ibid.

41 Interview with Expert 2. There are private and nonprofit efforts to catalog and distribute decryption keys as well, like No More Ransom, which, according to their website, is "an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky and McAfee with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals." Incident response plans should include a check-in with No More Ransom to attempt to secure keys. See No More Ransom at https://www.nomoreransom.org/en/index.html.

42 "Ransomware Guide," Stop Ransomware, Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/stopransomware/ransomware-guide.

43 Rogers, "Ransomware Management and Recovery Tactics."

44 Interview with Expert 3.

45 Lang, "Kaseya Ransomware Reaction."

46 "Sonoma Valley Hospital Suffers Significant EHR Downtime Event," HIPAA Journal, October 28, 2020, https://www.hipaajournal.com/sonoma-valley-hospital-suffers-significant-ehr-downtime-event/.

47 "Sonoma Valley Hospital Notifies Patients Affected by Ransomware Attack," Sonoma Valley Hospital, December 10, 2020, https://www.sonomavalleyhospital.org/sonoma-valley-hospital-notifies-patients-affected-by-ransomware-attack/.

48 Eshelman, "The Anatomy of a Targeted Industrial Ransomware Attack."

49 Austin, "This Company Was Hit with a Devastating Ransomware Attack."

50 Briggs, "Hackers Hit Norsk Hydro."

51 Emily Harding et al., "Never Trust, Always Verify": Federal Migration to ZTA and Endpoint Security," CSIS, *CSIS Briefs*, June 16, 2022, "'Never Trust, Always Verify': Federal Migration to ZTA and Endpoint Security," CSIS, *CSIS Brief*, June 16, 2022, https://www.csis.org/analysis/never-trust-always-verify-federal-migration-zta-and-endpoint-security.

52 Ransomware Task Force, *Combatting Ransomware*, 81.

53 HSGAC, *America's Data Held Hostage*, iv.

54 Emily Harding, "Holding Moscow Accountable for Its Criminal Networks," CSIS, *Commentary*, June 1, 2021, https://www.csis.org/analysis/holding-moscow-accountable-its-criminal-networks.

55 Chad Hemenway, "Court Siding with Merck over War Exclusion for Cyber Attack a Warning to Insurers," Insurance Journal, Februar 4, 2022, https://www.insurancejournal.com/news/national/2022/02/04/652272.htm.

56 Ibid.

57 Heather Howell Wright and Andrew Tuggle, "Four New Cyber War Exclusions from Lloyd's Market Association, National Law Review, January 10, 2022, https://www.natlawreview.com/article/four-new-cyber-war-exclusions-lloyd-s-market-association.

58 Josephine Wolff, "Who Pays for an Act of Cyberwar?," *Wired*, August 30, 2022, https://www.wired.com/story/russia-ukraine-cyberwar-cyberinsurance/.

59 Hemenway, "Court Siding with Merck."

60 HSGAC, *America's Data Held Hostage*, 32, 39, 42–43.

61 Ibid., 42.

62 Interview with Expert 1.

63 "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," CISA, https://www.cisa.gov/circia.

64 "Cyber Risk," Moody's 2021–2022, https://www.moodys.com/newsandevents/topics/Cyber-Risk-00704E.

65 Expert 2.

66 Expert 4.

67 Ibid.

68 Ibid.

69 Interview with Expert 2.

70 U.S. Department of Justice, *FYs 22-2026: Strategic Plan* (Washington, DC: DOJ, updated July 2022), https://www.justice.gov/doj/book/file/1516901/download.

71 "Blueprint for Ransomware Defense," Institute for Security and Technology, https://securityandtechnology.org/ransomwaretaskforce/blueprint-for-ransomware-defense/

72 Interview with Expert 1.

73 Ibid.

74 Eshelman, "The Anatomy of a Targeted Industrial Ransomware Attack."

75 HSGAC, A*merica's Data Held Hostage*, 42.

76 Rogers, "Ransomware Management and Recovery Tactics."

77 Ibid.

78 Expert 5.

79 "Preparing for a Cyber Incident – A Guide to Ransomware," U.S. Secret Service Cybercrime Investigations, https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident.

80 Austin, "This Company Was Hit with a Devastating Ransomware Attack."

81 Briggs, "Hackers Hit Norsk Hydro."

**COVER PHOTO** ANDREY POPOV/ADOBESTOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**