LAWFARE

FOREIGN POLICY ESSAY

Ransomware Lessons for a Nation Held Hostage

By **Danielle Gilbert** Sunday, September 12, 2021, 10:01 AM

Editor's Note: *The ransomware threat is growing, and policymakers and corporate America alike are wrestling with how to manage it. However, ransoms are not new, and, indeed, the United States has a long track record on this painful issue. The Air Force Academy's Danielle Gilbert examines ransomware with this track record in mind, drawing on the history of hostage-taking to identify ways to manage this problem.*

Daniel Byman

***

"Hold on, is it just me or did there not used to be a massive ransomware attack every two months?" In a recent episode of "Last Week Tonight," host John Oliver confronted the apparent explosion of ransomware incidents. These attacks, which involve infecting a digital device like a smartphone or computer with malicious software and encrypting and/or threatening to release data until a ransom is paid, have been around for 20 years. But they have recently reached a fever pitch, as perpetrators have targeted critical infrastructure and exponentially increased their demands. This year alone, ransomware attacks disrupted the largest oil pipeline in the United States and the meatpacking plant responsible for a fifth of America's beef; one ransomware gang carried out the largest attack on record, demanding $70 million to unscramble devices in 17 countries. Attacks on hospital systems and local governments are as devastating as they are common: Software company Emsisoft reported that 2,354 local governments, health care facilities and schools in the United States were hit with ransomware in 2020—a figure almost certainly dramatically underreported.

Ransomware may be new, but hostage-taking is not. For decades (if not centuries), the United States has had a hostage problem. From the Barbary pirates to Bowe Bergdahl, hostage crises have attracted tremendous media attention and fundamentally altered U.S. policy. Long after the embassy and hijacking waves of the 1970s, hostage-taking violence remains an intractable problem for international security. According to the former director of the FBI's interagency Hostage Recovery Fusion Cell, "Not a week goes by without the kidnapping of an American citizen abroad."

The past half-century of hostage-taking provides valuable lessons for understanding and confronting ransomware attacks. The similarities between these two forms of coercion—and ransomware's problematic departures—can tell us a lot about the dynamics at play. The successes and failures of U.S. hostage policy can help evaluate the policy options on the table for this new threat.

The Power to Hurt

Hostage-taking and ransomware are both strategies of coercion that leverage captivity to demand concessions. While not hostage-taking in the strictest sense—no people are being held—ransomware highlights what Thomas Schelling called "the power to hurt." It asks targets to trade concessions for the prevention of prospective pain.

Both hostage-taking and ransomware attacks create a bilateral monopoly: a false market in which there is only one seller (the perpetrator) and only one buyer (the target). The perpetrator can thus take advantage of built-in price insensitivity to make exorbitant demands and expect them to be met, raising ransoms to tens of millions of dollars. These attacks are useful to make money, yes—but also to highlight vulnerabilities in the system or embarrass an adversary. Famous hostages like American heiress Patty Hearst and Colombian presidential candidate Ingrid Betancourt attract attention to their captors and challenge the state's monopoly on violence.

These famous cases suggest that hostage-takers seek publicity—and many do. But the vast majority of hostage-taking and ransomware attacks transpire in secret. Targets may wish to avoid the reputational hit of looking insecure. They may also shun publicity so that they can make concessions without fear of reprisal. Some notorious kidnapping hotspots have imposed legal hand-tying mechanisms to prevent targets from paying ransoms, hoping to disincentivize hostage-taking in general and otherwise reduce its frequency. In Colombia and Italy, for example, anti-kidnapping legislation freezes families' assets when they report a kidnapping to law enforcement. Such policies disincentivize reporting.

Further, both state and non-state actors can take hostages or employ ransomware. While kidnapping has traditionally been the purview of criminal and political armed groups, states including China, North Korea, Turkey and Iran have engaged in hostage diplomacy—holding foreigners hostage for leverage under the guise of law. Some states condone hostage-taking by providing safe havens for captivity. These state protections are a major driving force of ransomware attacks, as Russia protects (and perhaps employs) hackers to commit these crimes abroad.

In all of these ways, ransomware resembles the hostage-taking violence of the past. What began as the malicious control of data for profit has, in recent years, brought human lives into the balance. Attacks on critical infrastructure highlight how digital attacks manifest in the physical world; attacks on hospital systems could credibly kill. As ransomware comes even closer to holding humans hostage, its innovations make it even harder to prevent.

What Makes Ransomware Different

Ransomware is the latest in a series of hostage-taking paradigm shifts fueled by new technology. For example, the growth of commercial air travel in the mid-20th century helped fuel a wave of airplane hijackings in the 1960s and 1970s. The rise of smartphones and portable internet technology in the early 2000s fueled a shift in hostage-taking from the public to the clandestine. The ability to produce and disseminate spectacularly violent hostage videos from a position of relative safety meant that perpetrators no longer had to negotiate their way out, or die trying.

Two new technological shifts make ransomware especially attractive for perpetrators, with no equivalent benefit accruing to the targets. First, cryptocurrencies make for safe and easy ransom payments. Before the advent of cryptocurrency, kidnappers collected ransom during a "drop"—when the target delivers the agreed-upon sum at the time and location of the kidnapper's choosing. The drop is dangerous for kidnappers, because it may provide an opening for law enforcement to trace or capture the perpetrators. Traditional wire transfers also prove risky, as such transactions are easily traced. But paying ransoms in cryptocurrency solves both problems for perpetrators by eliminating the physical and informational risk to getting paid. Cryptocurrencies' digital, unregulated and largely anonymous nature make them exceptionally useful for perpetrators.

Second, "malware-as-a-service" obviates the need for the skilled and specialized team at the heart of every hostage-taking. From Afghanistan to Ann Arbor, hostage-takers rarely act alone. One of the most consistent elements of hostage-taking plots is the role specialization among cells of 10-15 perpetrators, in which different actors are responsible for gathering intelligence on the target, executing the abduction, protecting the group and negotiating the hostage's release. This dynamic changes dramatically with off-the-shelf ransomware and malware services widely available for purchase. In other words, pretty much anyone can commit a ransomware attack, regardless of whether they have the skills and knowledge about how to do so. The proliferation of malware-as-a-service has precluded the need to learn special skills before exercising them and invites lone wolves to wreak tremendous havoc.

Lessons From U.S. Hostage Policy

Over the past 50 years, attempts to curb hostage-taking have taken distinct approaches, with varying efficacy. As the White House launches a new task force on ransomware and releases resources for businesses and communities, familiar debates about punishment have resurfaced. Past efforts to stop hostage-taking can teach valuable lessons for the ransomware fights ahead.

The first path is to take all possible measures to prevent ransomware in the first place. Countless articles provide the same straightforward list of ransomware prevention measures: segment networks, maintain backups, install security updates, secure passwords, implement multifactor authentication and train your team on cybersecurity measures. This advice is consistent and prolific, yet adoption is low.

Unfortunately, history suggests that preventive measures are difficult to realize and seem obvious only in retrospect. In the 1960s and 1970s, an airplane was hijacked every five and a half days. However, the commercial airlines were reluctant to impose new safety and screening measures on passengers, concerned that inconvenience would hurt business. Under these conditions, hijackings continued apace until airlines began X-raying luggage in the 1980s. Airport security isn't *fun*, but it has largely relegated hijackings to the past.

The second approach is what law enforcement and security personnel call "denial of benefits"—policies and tactics designed to prevent perpetrators from enjoying the fruits of their labor. This might mean, for instance, ensuring that hostage-takers receive ransom payments in a forged currency or recovering funds before the perpetrator can spend them.

"No concessions" policies are also designed to deny benefits to hostage-takers. These policies assume that perpetrators learn which targets won't pay and stop targeting them in the future. Existing research suggests that this is indeed the case—targets that paid ransoms yesterday are more likely to be kidnapped tomorrow than are those targets that refused. This is the logic behind calls to outlaw ransom payments to cyber criminals, including insightful and creative options published on this site. (That ransom payments are tax deductible, for instance, seems particularly egregious.)

Given their track record, however, such policies are both unwise and unlikely to curb ransomware attacks in isolation, for three central reasons. First, outlawing ransomware payments would represent a sea change to current U.S. ransom policies. Despite the well-known mantra that the United States has a "no concessions" policy, current law prohibits ransom payments only to the very limited list of U.S.-designated foreign terrorist organizations (FTOs). At the time of writing, it is perfectly legal for the U.S. government, businesses or individual citizens to make ransom payments to any other hostage-takers—be they foreign or domestic criminals, non-FTO armed groups or even states. We've relied on these payments to bring home hundreds of Americans kidnapped abroad. Outlawing ransom only when virtual would be inconsistent with current U.S. law, and could force a reckoning with decades of U.S. policy.

Second, a complete ban on payment is unlikely to work, because individual targets always have an incentive to cheat when their loved one's life (or their data) is on the line. At the national level, this could also have deleterious effects. As I've written elsewhere:

> In 2007, leaders of the G8 countries agreed to "stamp out" ransom payments to terrorist groups. However, in the subsequent decade, some G8 leaders would provide hundreds of millions of dollars in ransom payments to al-Qaeda and the Islamic State. This is particularly devastating when one perpetrator holds hostages from countries with diverging policies. For example, the Islamic State's French, German, Italian, and Spanish hostages were set free, while the American and British hostages were brutally killed. This suboptimal patchwork of legal regimes, in which some countries "take a hard line, and others are willing to talk," suggests the urgency of coordinated deterrence.

Third, punishing targets (rather than perpetrators) could result in substantial political backlash. In the United States, ransom payments to FTOs are outlawed through enforcement of Section 2339(B) of the material support statute: Paying a terrorist ransom comprises material support to a terrorist organization. In effect, this means telling families that rescuing their loved ones constitutes financing future terrorism. This came to a head in 2014 when the parents of Islamic State captives James Foley, Steven Sotloff, Peter Kassig and Kayla Mueller pleaded with the White House to rescue their captive children. As the surviving Foleys told ABC News, they were threatened repeatedly by a military officer on the White House's National Security Council staff and a State Department official: Pay, and you will be prosecuted as criminals.

Translating this dynamic to ransomware, it's easy to imagine significant political backlash for threatening—or actually punishing—sympathetic victims of a crime. As targets shift from tech companies to critical infrastructure, lives will hang in the balance. Policymakers would be wise to think hard before placing the onus on victims to stop these attacks.

Instead, anti-ransomware policy should focus on punishing the perpetrators. Some existing hostage recovery policies crack down on perpetrators directly through specialized units designed to disrupt hostage-taking attacks. In the United States, this looks like the FBI's Hostage Rescue Team and two military Special Forces units—the Army's Delta Force and the Navy's SEALs—which relentlessly train to disrupt hostage crises around the world. In Colombia, specialized units in both the police and army focus exclusively on hostage-taking; they have been credited with driving the dramatic reduction in Colombian kidnapping over the past 20 years.

Recent news suggests that impending crackdowns have already had an effect on perpetrators, but more should be done. The White House has advanced initiatives to shore up cybersecurity, including a ransomware task force, a website highlighting preventive resources and the "Rewards for Justice" program. But without serious investment in the FBI's ability to investigate and intervene, perpetrators will continue to attack the least secure among us.

In the absence of clear and consistent policies, responses to hostage-taking highlight the importance of enacting harm mitigation techniques. A robust hostage response industry—including kidnap and ransom insurance agents and private hostage negotiators—brings skills, experience and maxims to regularize the market. Their role has largely focused on underwriting the costs of kidnapping to the target and mitigating harm, facilitating hostage recovery while making attacks more time consuming and less profitable for perpetrators.

Two approaches to harm mitigation seem promising. First, professional hostage negotiators advise targets to never pay the initial ransom demand but, rather, to counter and negotiate a lower price. Hostage-takers typically demand more money than they expect to receive; when targets pay immediately, perpetrators infer that they haven't asked for enough. At the very least, making a credible counter-offer might curb the exponential increase in ransomware demands.

Second, it is costly to hold a hostage in the real world: Perpetrators must have the resources to feed, clothe and hide their prisoner throughout captivity, while protecting their group from counterinsurgency or policing. Operating in the digital realm (and with Russian safe harbor), such costs are less likely to translate. But delay tactics might offer law enforcement a greater opportunity to intervene or allow targets to come up with alternative solutions to recovering their data. Time—or other factors to increase perpetrators' costs—can mitigate the harm to victims.

In recent years, policymakers have adopted legislation and established interagency efforts to address hostage-taking directly and comprehensively. An equivalent focus on ransomware must operate on all fronts: bolstering the FBI's ability to trace and recover ransoms; confronting the challenges of cryptocurrency and Russian safe harbor; and securing the most vulnerable health, energy, food, water, transportation and emergency sectors from attack. Failure to do so risks holding the future hostage.

Topics: Foreign Policy Essay

Tags: ransomware

Danielle Gilbert is an assistant professor of military and strategic studies at the U.S. Air Force Academy, a nonresident fellow with the Modern War Institute at West Point and a fellow with the Bridging the Gap Project. Her research focuses on the causes and consequences of hostage-taking violence. The views expressed are the author's and do not represent the U.S. Air Force Academy, the Department of the Air Force or the Department of Defense.

@_danigilbert