Ransomware attacks are about to get worse. But there are ways to stop them

Opinion by Matthew F. Ferraro for CNN Business Perspectives
Updated 11:20 AM ET, Mon September 13, 2021

Editor's Note: *Matthew F. Ferraro is a former intelligence officer, a counsel at WilmerHale, a term member of the Council on Foreign Relations and a visiting fellow at the National Security Institute at George Mason University. The opinions expressed in this commentary are his own.*

The September 11 attacks demonstrated, with horrifying clarity, the outsize power individuals have to wreak havoc on an open society. Since that awful day, the spread of technology and our solidifying interconnectedness have increasingly placed the capacity for disruption and harm in the hands of not just states, but of individuals all over the globe. This trend has been called the democratization of violence, and it describes literal, kinetic violence (think bioweapons cooked up in a kitchen and mini-drones weaponized in a garage) and less physical but still devastating cyberattacks.

These threats will continue to grow in the months and years ahead because cyberattacks of all kinds are relatively cheap and can be launched at scale. Now, American industry and government must work more closely together to buttress the defenses necessary to thwart these attacks.

Ransomware is the latest example of the "democratization of violence" trend. In a ransomware attack, a bad actor accesses a victim's computer system, uses malware to encrypt the system's data, and only decrypts it if the victim pays a ransom, usually in Bitcoin because it is difficult to trace. Anyone with an internet connection — from nation-states to criminals to terrorists — with minimal skills and malevolent intentions can now launch these attacks thanks to the advent of "ransomware as a service." In this business model, ransomware developers lease pre-made malware to anyone who pays, and the developer gets a cut of the ransom payments.

Ransomware extortions have become a self-sustaining ecosystem of criminality. It is a thriving business because most victims are willing to pay relatively modest ransoms, which then fund further attacks. Paying a ransom

may incentivize bad behavior, but a victimized company usually (and understandably) just wants its data back as quickly as possible.

Hackers are most often after money, but attacks can also destabilize the US economy, whether intentional or not. For example, in May 2021, a hacking group called DarkSide launched a ransomware attack against Colonial Pipeline, one of the largest fuel pipelines in the United States, forcing a shutdown of its fuel distribution operations across several states. Consider what kind of physical assault it would have required 20 years ago, in a pre-cyber era, to set off a wave of gas shortages across the eastern part of the country.

The scale and impact of these attacks have exploded in recent years. According to one estimate, ransomware will cost the global economy approximately $20 billion in 2021, a 57-fold increase from 2015. Everyone is vulnerable.

In short, America's cybersecurity system is blinking red. President Biden signed an executive order back in May that requires software sold to the government to meet baseline security standards, demands federal contractors swiftly report cyber incidents, and creates a National Transportation Safety Board-like government entity to review major breaches.

The White House is also calling on the private sector to do more to address cybersecurity, what President Biden called a "core national security challenge" during a recent meeting with tech titans. The administration subsequently announced a number of government and private sector initiatives, including a collaboration to develop a new framework to improve the security of the technology supply chain, increased efforts to train a diverse cybersecurity workforce, and the expansion of an Industrial Control Systems Cybersecurity Initiative from electric utilities to natural gas pipelines, among others.

These are all welcome moves, but there is much more the government and industry can do:

First, the government should act where businesses cannot and take all actions within its power to disrupt the ransomware activities of foreign states and their criminal gangs. That means employing diplomatic pressure, tying progress on taking ransomware groups offline to sanctions relief to the countries where the groups reside, indicting bad actors overseas, extraditing and prosecuting them, and (potentially) taking offensive cyber action against ransomware groups.

Second, the Biden administration should incentivize companies to prepare for ransomware by setting out specific guidelines for what businesses should do to prepare for and respond to ransomware attacks. Right now, the government speaks out of both sides of its mouth. Its official position is that companies should not pay ransoms, but it recognizes that it is often in the company's — and the public's — best interest to pay. The FBI urges victims to coordinate with law enforcement about ransomware incidents and to share if ransom has been paid, and through what Bitcoin address.

This ambiguity makes it harder for businesses to manage ransomware risks because they are unsure what steps they should take to navigate these issues, and it leaves them open to post-ransomware litigation. Indeed, Colonial Pipeline was hit by at least two lawsuits after it was victimized. If the administration doesn't establish such standards now, it will be left to the courts to do so as they resolve these types of suits.

Third, the government should work with companies that are victims of ransomware attacks to recover cryptocurrency paid to hackers, thus interrupting the cycles that fund future attacks. Notably, the FBI worked with Colonial Pipeline to seize over $2 million of Bitcoin paid to the hackers, in a promising sign of what may come from the Department of Justice's recently established Ransomware and Digital Extortion Task Force. As the Deputy Attorney General Lisa Monaco said, "Following the money remains one of the most basic, yet powerful tools we have."

None of these actions will eradicate the business risks of ransomware, but they can help counter the democratization of violence with a culture of common defense.

URL: https://www.cnn.com/2021/09/13/perspectives/ransomware-attacks-cybersecurity/index.html