November 8, 2021

Enough with the Sticks: Why It's Time for Policymakers to Embrace Carrots in the Fight Against Ransomware

by Anthony D. Glosson

In the world of ransomware response, one resource is becoming increasingly indispensable: the federal government. The FBI, in particular, is often able to provide deep expertise in specific ransomware variants and the threat actors behind them, leveraging insights gleaned from investigations of attacks across the country that in many cases far exceeds anything available to a single consultant or security team. From a public policy perspective as well, there's a strengthening consensus that cyber threat information sharing, such as that coordinated by the federal Cybersecurity and Infrastructure Security Agency, represents some of the lowest-hanging fruit in designing a more secure internet and facilitating greater resiliency for banks and other commercial enterprises.

Policymakers at the federal and state levels, however, risk undermining this public-private cooperation and turbocharging the ransomware menace with the wrong kind of ransomware legislation introduced across the country just this year, including information sharing mandates, prohibitions on ransom payments, and other prescriptive rules tying the hands of breach response professionals responding to a cybersecurity crisis.

Take New York S6806A for example, which stipulates that "no [business] shall pay, or have another entity pay on their behalf, ransom in the event of a . . . ransomware attack." Other state legislatures are considering similar anti-ransom bills, including Texas, North Carolina, and Pennsylvania. This "no-concessions" strategy is an age-old one, marshalled by governments around the world to deter piracy and kidnappings. After all, if outlaws cannot make money by literal or proverbial hostage-taking, they are less likely to keep taking hostages.

But bans on cybersecurity ransom payments are a cure worse than the disease. Unlike piracy and kidnapping, ransomware distribution is a low-overhead numbers game for threat actors, meaning that they are unlikely to simply stop taking digital hostages from jurisdictions with ransom payment bans.

More importantly, ransom bans give cyber criminals yet another bite at the extortionary apple. As my colleague Jon Neiditz explains in the adjacent pages, ransomware threat actors already have two pressure points by which to demand payment: the loss of crucial business data and the sale or publication of that data. To these, ransom bans would add a third: the threat of prosecution for banks and other organizations that play ball to protect their business records—and their customers' personal information. After receiving a ransom payment, cyber criminals could circle back and threaten to report that payment to local authorities unless the victim makes still further "hush money" payments. This messy state of affairs would make victims less likely to coordinate

with law enforcement in the first place, disrupting the virtuous cycle of public-private information sharing that has proven to be so valuable to breach prevention and response.

There is a better way. Rather than driving a wedge between private businesses and public authorities with threats of punishment for ransom payments or insufficient information sharing, policymakers should incentivize public-private cooperation through positive reinforcement—carrots, not sticks. For example, policymakers should consider incentives like the following ones:

- Special privilege for information disclosed to the FBI and other authorities assisting with breach response and prosecution. State attorneys general and federal regulators, for example, should not be able to use such information as grist for data security enforcement actions. Regulators could continue to enforce data protection laws through ordinary means, but authorities who receive ransomware attack information in confidence should be legally obligated to maintain it in strict confidence.
- Clear security standards with safe harbors that provide certainty to compliant businesses that they will not face legal repercussions for having been the victim of a breach. These standards should scale appropriately with the size of a business; a community bank should not be held to the same standards as a multinational financial behemoth.
- Legal protection for strong encryption technologies at the federal level, including a clear statutory prohibition on any federal or state mandates that would require tech service providers to build in backdoors for law enforcement to bypass encryption.
- Budgets to promote awareness of law enforcement expertise and other available resources for businesses experiencing ransomware attacks.
- Acknowledgment of the frequent necessity of ransom payment and resources for evaluating options and insurance coverage and assurance that coordinating with law enforcement will not preclude the payment of a ransom.

Cybersecurity legal standards notoriously lag behind the threat landscape, but by ditching the stick and embracing realistic, incentive-based collaboration, policymakers can contribute to more secure transactions and help disarm threat actors in the process.