Client Update
New Federal Ransomware Guidance

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Mark P. Goodman
mpgoodman@debevoise.com

Maura K. Monaghan
mkmonaghan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

David Sarratt
dsarratt@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

The U.S. Department of Health and Human Services (HHS) has just issued significant new guidance on ransomware. The guidance makes clear that entities subject to the data security provisions of federal healthcare law now have specific responsibilities both to guard against ransomware attacks and—in a departure from existing breach notification requirements—to report such attacks when they happen. Given that ransomware attacks are spiking sharply across corporate America, the HHS guidance is instructive not just for healthcare entities but for enterprises in all sectors.

RANSOMWARE FAQ

What is ransomware? Ransomware is a form of attack where the hacker does not steal your files, but encrypts them so you cannot access them. Then the hacker offers to sell you the encryption key, typically payable in the online currency Bitcoin. The usual demand comes with a deadline—after which time, the hacker threatens, the key will be discarded and your files will remain forever inaccessible.

If a low-tech metaphor helps: Think of the ransomware attacker as a sort of reverse "burglar," who doesn't break in to your house, but locks you out of it and demands payment to let you back in.

Why is the government taking action? Ransomware attacks are way, way up. There have been an estimated 4,000 attacks a day in 2016 to date, representing a 300% increase over 2015. Historically, ransomware attacks tended to be petty crimes directed at individuals and mom-and-pop organizations. But these attacks are now being directed more often, and with more success, at larger enterprises.

How do ransomware attacks happen? Ransomware gets onto an enterprise's system like any other kind of malware. "Phishing" attacks, where users

unwittingly click on a malware-laden link or attachment in a seemingly innocent email, are a common vector. Hackers also may steal system credentials or exploit software vulnerabilities to install ransomware.

Hackers who successfully launch their ransomware then typically post threatening messages on the screens of users at the victim entity. In one example cited by the Department of Justice, the hacker asserted that the users themselves had engaged in illegal activity and must pay a "fine." In another, the hacker stated that a ransom must be paid within a certain time period or "all your files will be permanently encrypted and nobody will be able to recover them."

Do victims pay the ransom? Often, yes. No comprehensive metrics are publicly available, but at least one study reports a 40% pay-up rate. It is a matter of public record that, earlier this year, Hollywood Presbyterian Hospital in Los Angeles paid its hacker 40 bitcoin, or about $17,000. Even law enforcement is not immune; a Massachusetts police department has admitted that it paid a ransom to retrieve its work files.

Why pay? In that memorable line from the movie "Argo," payment of the ransom may be the victim's "best bad option." Enterprises face a tough choice when the encryption is not defeatable and the padlocked files are business-critical. (How long can a modern hospital, for example, be offline before devastating consequences occur?) Compounding these difficulties, law enforcement agencies generally cannot find the cybercriminal fast enough to satisfy business demands, if they can find the criminal at all. (He may be overseas.) Moreover, the bad guys frequently set the ransom at or about nuisance-value levels. And at least until now, there has been no disclosure requirement.

Add it all up, and payment of the ransom—however frustrating—can seem to be a reasonable cost-benefit calculation. As one FBI official has said, "To be honest, we often advise people just to pay the ransom." (To be clear, the FBI's official policy is that victims should contact law enforcement. The new HHS guidance calls for reporting of ransomware attacks to the local FBI or Secret Service field office.)

Do hackers who are paid actually supply the encryption key? Often, yes. Again, metrics are hard to come by—but an FBI source has said that typically, "You do get your access back." Some ransomware attackers even ask you to rate them, like an Uber driver, so they can advertise to future victims that they have a track record of supplying the encryption key once paid.

There is not always honor among thieves. Published reports indicate that just this spring, a hospital in Wichita paid a ransom—but in return got only partial access to its files, together with a demand for an additional payment.

Isn't ransomware a crime? You bet. At a minimum, ransomware schemes run afoul of the federal computer crime statute, 18 U.S.C. § 1030, and particularly subsection (a)(7), which forbids hacking intended to extort something of value from the victim.

Up to now, what have been the legal obligations of ransomware victims? Few, if any:

- Most states have laws requiring disclosure of data breaches, but these laws ordinarily kick in only when data containing personal information is exposed or stolen—not when the data is simply made inaccessible.
- In specific situations, companies may be contractually required to give notice to their counterparties of certain cybersecurity events, including ransomware attacks.
- The U.S. Federal Trade Commission generally takes the position that maintaining poor cybersecurity can be an unfair business practice under Section 5 of the FTC Act. But the FTC has not yet applied this theory to try and hold a ransomware victim culpable. Informally, the FTC has indicated that it is focused on hacking cases that cause large-scale consumer impact—a description that does not fit the classic historical ransomware case, but might fit the emerging breed of enterprise-level ransomware attack.

THE NEW HHS GUIDANCE

The federal Health Insurance Portability and Accountability Act (HIPAA), has long imposed cybersecurity standards on covered entities and their business associates via the HIPAA Security Rule. The new July 11 guidance makes clear that HIPAA's cybersecurity standards will now be construed to apply to ransomware.

First, the guidance makes clear that those subject to HIPAA must "implement policies and procedures that can assist an entity in responding to and recovering from a ransomware attack."

These policies and procedures should include "maintaining frequent backups" and conducting periodic "test restorations," *i.e.*, measuring the enterprise's ability to actually function from backups if a ransomware attack were to limit access to

regular systems. HHS also counsels organizations to "consider maintaining backups offline and unavailable from their networks." This is because of the propensity of ransomware attackers to target the backup files themselves—in effect, padlocking the garage door as well as the front door.

The HHS guidance specifies that all this is part of the larger obligation, under the Security Rule, to maintain a "data backup plan" that includes provisions for disaster recovery planning, emergency operations, analyzing the criticality of applications and data, and periodically testing contingency plans.

The long-standing HIPAA mandate to maintain "security incident procedures" will now be construed to require processes that will allow an organization to detect, analyze, contain, eradicate and recover from a ransomware attack. Ransomware attacks are now explicitly defined as "security incidents" triggering the obligation to deploy these procedures. Likewise, the long-standing requirement that a covered organization's workforce must receive appropriate security training now includes a requirement that the workforce be trained in how to detect and report malware so as to help ward off ransomware attacks.

Second, breach notification obligations may well now kick in under HIPAA even if other notification triggers, such as the states' notification statutes, are not implicated. The guidance is quite clear that "the presence of ransomware . . . is a security incident" for purposes of the Security Rule, and qualifies as a breach because unwanted encryption of personal health information (PHI) by the ransomware attacker amounts to "acquisition" of that data by the attacker within the meaning of the Rule. Until now, ransomware and the payment of a ransom typically did not trigger breach disclosure obligations, and the guidance marks a significant departure from prior practice which may be a harbinger of change in other sectors.

Whether HIPAA disclosure procedures must be followed will be a case specific determination. But the general rule is that disclosure must occur unless the enterprise can show a "low probability" that PHI has been compromised. Traditional factors in this analysis include the nature and extent of PHI involved, whether the PHI was actually acquired or viewed, and the extent of risk mitigation. Under the new guidance, a "high risk of unavailability of the data, or high risk to the integrity of the data" is to be considered an indicator of compromise.

If the data encrypted by the ransomware attacker was previously encrypted by the data holder, that may cut against disclosure being required. Even then, though, the determination is case-specific—for example, a ransomware attack on

an encrypted laptop could still result in a breach, for purposes of the Security Rule, if "the file containing the PHI was decrypted and thus 'unsecured PHI' at the point in time that the ransomware accessed the file."

WHAT'S AN ENTERPRISE TO DO?

Organizations subject to HIPAA of course must sit up and take notice of the new HHS requirements, and review their training programs, technical protections, backup systems and incident response protocols for compliance with the new guidance.

Organizations in all sectors of the economy can learn from the HHS requirements, however, and by doing so can reduce both their business and legal risks associated with ransomware. For it seems safe to say that once a major agency like HHS defines an obligation to detect, prevent, combat and report ransomware attacks, then other legal authorities may converge around similar views.

The Department of Justice, the Secret Service and other federal agencies have joined with HHS to issue best-practices guidance for all enterprises. The interagency guidance is not limited to healthcare entities, and it closely resembles the new HHS mandates for HIPAA-covered organizations.

Also part of the chorus is the federal Computer Emergency Response Team (US-CERT), a technical expert entity based at Carnegie-Mellon University that recently issued its own guide, Ransomware and Recent Variants. CERT's guidance on risk mitigation closely resembles the interagency recommendations and HHS mandates.

Ransomware thus joins the growing list of cybersecurity threats that, under the law, potential victims are well advised to take specific measures to prevent, detect and mitigate.

* * *

Please do not hesitate to contact us with any questions.