Client Update
Global Ransomware Attack: Essential Steps to Manage the Risks

WASHINGTON, DC
Luke Dembosky
ldembosky@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

James J. Pastore
jjpastore@debevoise.com

Stephanie M. Cipolla
smcipolla@debevoise.com

LONDON
Jane Shvets
jshvets@debevoise.com

Robert Maddox
rmaddox@debevoise.com

HONG KONG
Mark Johnson
mdjohnson@debevoise.com

MOSCOW
Anna V. Maximenko
avmaximenko@debevoise.com

As has been widely reported, a wave of ransomware attacks struck organizations around the world late last week, locking users out of their computer files unless and until they pay the hackers a ransom in Bitcoin. The attacks were alarming both because many hospital systems were heavily impacted, particularly in the U.K., and because of how rapidly they spread around the globe. The attacks are a reminder that organizations can and should take specific steps to address ransomware as part of their broader cybersecurity programs. Taking such steps is both good common sense and, increasingly, a legal mandate.

WHAT HAPPENED?

The attacks reportedly exploited a recently announced Windows vulnerability that a hacking group known as Shadow Brokers claimed to have stolen from the U.S. National Security Agency. Microsoft had released a patch for newer versions of its operating systems in April, but no patch was available for older operating systems on which many hospitals and others were running, such as Windows XP, until after the attacks commenced. Those who had failed to patch their systems, or who were running old operating systems, were vulnerable. The hackers behind this sadistically named their exploit the "WannaCry" or "WannaCrypt" ransomware.

As of today, public reports indicate over 200,000 victims of WannaCry ransomware in 150 countries. Russia, Ukraine, and Taiwan are the most heavily targeted countries to date, but the victims also include major institutions elsewhere, such as the National Health Service in the U.K. and Telefónica, the Spanish telecommunications company.

HOW BEST TO PREPARE AND RESPOND

Preparation for these incidents requires a combination of technical, legal and practical steps. As lawyers, we are not purporting to advise you on specific

technical measures. We do encourage internal counsel who "own" cybersecurity issues to promptly incorporate, or refresh, the discussion of ransomware as part of their ongoing dialogue with information security colleagues.

- **Patch your systems:** The immediate priority should be to patch your systems. You can do so directly at Microsoft's website. Make sure you perform any downloads from the actual Microsoft site by going there directly, and not in response to any unsolicited email you may have received containing a link to install a patch.
- **Back up your data:** It is vital that your systems are backed up frequently and in a careful manner to prevent the ransomware from encrypting your backups as well. Attackers know that you will look to your backup systems to try to recover your files, and therefore commonly also try to lock you out of the backups to keep you on the hook to pay the ransom. Keep in mind that files saved only locally on infected systems are likely to be lost.
- **Immediately alert your employees:** "Phishing" emails, which attempt to trick the recipient into clicking on a malicious link or opening an attachment laced with malicious software or "malware," are a major attack vector for the spread of ransomware. Some early reports say that WannaCry has spread in part through phishing emails containing encrypted attachments. You should immediately remind your employees – as well as contractors who have access to your network – to be on high alert for emails, particularly with links or attachments, from unknown sources or that appear to be from known sources but include unusual requests. Although technical experts believe that WannaCry spreads in an automated fashion once inside a victim's network, the initial compromise of the network likely comes from a phishing email.
- **Assess your defenses:** Evaluate your technical defenses with advice from both technical and legal experts. This includes, among other things, deploying updated antivirus at system endpoints, installing firewalls to filter malicious traffic, using network segmentation to stop or slow the spread of any infection, and using intrusion detection software to provide timely alerts of unusual traffic within your network.
- **Train for the worst:** Practice working through a ransomware scenario and how you would respond, including what legal, technical and broader business choices you would make. Drills should include a simulated re-start of your network using your existing backup systems, to help you assess how fresh and reliable those backups are as well as how quickly you can work around a ransomware attack by operating from the backups. This also provides an opportunity to consider whether certain key parts of your network or

backups should be technically separated so that ransomware cannot spread to them.

We often include ransomware scenarios in response drills, a/k/a tabletop exercises, to help our clients become efficient at responding to and managing these and other incidents. If your organization does not have a written cyber incident response plan ("IRP") that it tests regularly, now is a good time to begin adopting one. Given that speed of response is essential, the IRP, combined with testing, is a vital tool in avoiding any wasted time in escalating a potentially serious incident to the right personnel.

- **Line up outside help:** Arrange in advance the outside technical incident response vendor(s) you would use, and consider putting their retainer in place through outside counsel to have the best chance of establishing privilege over investigation of and response to the incident. Many of our clients have these arrangements in place in advance so they do not waste precious time looking for, evaluating and engaging outside help during the storm of an incident.
- **Know your investigator:** To be ahead of the curve, you should know the face and cell phone number of the FBI, Secret Service, National Crime Agency or other law enforcement officials you would call with an urgent cybersecurity matter. Before you call, however, you should discuss with experienced in-house or outside counsel the pros and cons of engaging law enforcement and how to handle the interaction effectively. We often use our extensive law enforcement experience and relationships to help broker these discussions on behalf of our clients.
- **Assess insurance:** Assess your cyber insurance policy and refresh your understanding of the scope of coverage and the notification requirements it contains.
- **Stay current:** Stay on top of the latest cyber threats by participating in an industry platform such as an Information Sharing and Analysis Center ("ISAC") with members from your industry sector or an Information Sharing and Analysis Organization ("ISAO") that has members across sectors. The Financial Services ISAC or "FS-ISAC" is one example. More information is available through the National Council of ISACs.
- **Consider potentially required disclosures:** Although ransomware does not typically steal personal consumer data, the disruption it can cause to system operations may trigger contractual or regulatory notifications, depending on the nature of the business and its regulatory environment.

- **Pause before you pay:** In the event that your organization suffers a ransomware attack and you are faced with the choice of whether to pay a ransom, consult counsel regarding the potential legal and practical ramifications of the decision. Many organizations do choose to pay because the files the attacker has "padlocked" are business-critical and because the ransom amounts often are set at nuisance levels. But this choice is not without risks that you should consider in advance. For example, if backups are insufficient to avoid a need to pay, there may be other technical alternatives available to obtain the password or "key" to unlock your files.

WHY IS RANSOMWARE A LEGAL ISSUE?

Preparing for ransomware is increasingly seen not just as good technical practice, but as a matter of legal obligation. As we have previously reported, all entities covered by the U.S. Health Insurance Portability and Accountability Act ("HIPAA") have specific duties to prepare for and respond to ransomware attacks under guidance from the U.S. Department of Health and Human Services ("HHS"). HIPAA-covered entities, for example, must treat certain ransomware attacks as triggering disclosure obligations to affected individuals and to government agencies.

HHS also has joined the Department of Justice and the Department of Homeland Security to issue best-practices guidance for the private sector generally. A number of recent post-breach court cases have cited the victim entity's failure to follow best practices as potential support for a negligence claim or other cause of action against it.

* * *

Avoiding, preparing for and responding effectively to a ransomware attack is part of a broader program of cybersecurity risk management and incident response. For questions or assistance, please do not hesitate to call on any member of the Debevoise Cybersecurity & Data Privacy global practice team.