crowell moring

CLIENT ALERT

A Ransomware Attack Primer: What You Need to Know and What Crowell Can Do to Help

Jun.17.2021

As recently as six months ago, ransomware was the domain of CISOs (chief information security officers) and cybersecurity lawyers. But in the wake of high-profile attacks by Russian-based cybercriminals on Colonial Pipeline, operator of the country's largest refined fuel pipeline, and JBS Foods, the world's largest meat processor, ransomware jumped to the top of the agenda for President Biden's meeting with Russian President Vladimir Putin this week. These high-profile incidents have shown that ransomware attacks are a significant business/operational and legal risk for global companies. Colonial Pipeline paid $5 million to resolve its attack, JBS $11 million, and the group responsible for an attack on Acer is demanding $50 million.

This is not just a matter of a few victims making the news. Security vendor Chainalysis reported a 311% spike in total amounts paid by victims in 2020 compared to 2019, with no signs the trend is slowing. Sophos recently reported that more victims are paying the ransoms and that attackers are increasingly coupling extortion with encrypting files, among other findings.

U.S. government officials have also made it clear that ransomware attacks now take their place alongside supply chain attacks, cyber-theft, and disinformation campaigns as a significant national security threat in the digital age. The DOJ announced the creation of a ransomware task force earlier this year in response to the surge of ransomware attacks during the pandemic. FBI Director Christopher Wray said the national security threat currently posed by ransomware is similar in scale to that of the terrorist attacks of September 11, 2001. According to the FBI Director, the Bureau is currently tracking close to 100 different types of ransomware, with many of the strains tied to criminal hackers in Russia. And the White House has emphasized the importance of industry taking immediate action to guard against ransomware attacks.

In light of these threats, the U.S. government has issued alerts and guidance, and is standing up task forces and other efforts focused on the threat. For example, a recent CISA alert sets out best practices for preventing business disruption from ransomware attacks, and the White House has also reportedly issued guidance to the private sector. Importantly, these actions represent more than just helpful advice; they are also likely defining what will be a new minimum standard of care that companies are expected to meet.

There may be other implications as well, such as potential sanctions and anti-money laundering (AML) risks associated with paying ransoms that are described in guidance from OFAC and FinCEN, respectively. The blockchain analysis company Chainalysis has estimated that 15% of all ransomware payments in 2020 went to attackers on the U.S. Office of Foreign Asset Control's sanctions list. Moreover, these ransoms are typically paid out in cryptocurrency, further increasing the sanctions and AML risks.

The good news is that, although ransomware incidents are increasing, they need not be catastrophic for a business. Rather, advance preparation, proper crisis management, timely remedial action, accurate assessments of harm, and, when appropriate, effective communications including notifications to government and affected individuals, can significantly mitigate the business impact of these incidents.

Crowell & Moring is well-positioned to help you prepare for and respond to ransomware attacks. In these crisis situations, our cybersecurity team is on the ground providing support at every stage, from initial internal investigation and risk management, through making notifications where appropriate, and, if necessary, government enforcement actions and litigation. We also work with technical consultants when appropriate through relationships structured to help maintain confidentiality and privilege for forensic investigations.

- REvil/Sodinokibi
- DarkSide
- Maze
- Ryuk
- Suncrypt
- DoppelPaymer
- Netwalker
- Cryptolocker
- SNAKE
- CL0P
- WannaCry
- NotPetya
- Multiple novel ransomware strains and emerging threat actor groups

Crowell & Moring's cybersecurity team also works closely with other practice groups at the firm that have relevant experience with the wide range of issues raised by ransomware attacks, including International Trade, Insurance/Reinsurance, Government Contracts, White Collar, National Security, and Financial Services.

If you need help assessing your ransomware preparedness or are the victim of an attack, please contact any of the Crowell & Moring lawyers listed below. We have also created a checklist for responding to a ransomware attack.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Michael K. Atkinson
Partner – Washington, D.C.
Phone: 202.624.2540
Email: matkinson@crowell.com

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Laura Foggan
Partner – Washington, D.C.
Phone: +1 202.624.2774
Email: lfoggan@crowell.com

Carlton Greene
Partner – Washington, D.C.
Phone: +1 202.624.2818
Email: cgreene@crowell.com

Michelle J. Linderman
Partner – London
Phone: +44.20.7413.1353

Email: mlinderman@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Matthew B. Welling
Partner – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com

David (Dj) Wolff
Partner; Attorney at Law – Washington, D.C., London
Phone: +1 202.624.2548, +44.20.7413.1368
Email: djwolff@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com