# CLIENT ALERT

## Don't be that Victim: The Critical Need for Ransomware Response Plans

**Jun.23.2021**

*Senator Maggie Hassan (N.H.-D): "My question is, in your planning, did you have a plan for cybersecurity response that included guidance about ransomware?"*

*Joseph A. Blount, Jr., President and Chief Executive Officer, Colonial Pipeline: "Senator, specifically, no, no discussion about ransom, and action to ransom."*

Senator Hassan's pointed question to Colonial Pipeline's Joseph A. Blount, Jr., before the Senate Homeland Security and Government Affairs Committee on June 8, 2021 underscored what many see as the key lesson learned in the wake of recent high-profile ransomware attacks on U.S. companies: it is essential to have emergency-response plans in place – beyond insurance policies – that specifically outline a company's response to a ransomware attack.

As we noted in our previous ransomware alert, 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.

As a result of the recent high-profile attacks on Colonial Pipeline and JBS Foods, government officials have made clear that ransomware attacks now take their place alongside supply chain attacks, cyber-theft, and disinformation campaigns as national security threats in the digital age. Indeed, the U.S. Department of Justice recently said that it was prioritizing ransomware investigations to a level similar to terrorism inquiries and requiring U.S. attorney's offices across the nation to coordinate ransomware investigations with a centralized ransomware task force. The DOJ had announced the creation of a ransomware task force earlier this year in response to the surge of ransomware attacks during the pandemic. "It's a specialized process to ensure we track all ransomware cases regardless of where it may be referred in this country, so you can make the connections between actors and work your way up to disrupt the whole chain," said John P. Carlin, principal associate deputy attorney general.

Relatedly, 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. In emphasizing the severity of the threat to U.S. companies presented by ransomware attacks, Wray made clear that the responsibility lay not just with government agencies, but also with the private sector.

The White House has also emphasized the importance of industry taking immediate action to guard against ransomware attacks. In a June 2, 2021 open letter to corporate executives and business leaders, Anne Neuberger, deputy assistant to the president and deputy national security adviser for cyber and emerging technologies, urged companies to follow the U.S. government's

best practices for addressing a ransomware attack, including backing up data, system images, and configurations; updating and patching systems promptly; testing incident response plans; and segmenting networks.

As the White House's letter notes, no company is safe from being targeted by ransomware, regardless of size or location. The hidden danger is that the ransomware attacks that will surface tomorrow are being executed today, and the one thing no company can buy with any guarantee when it comes to a ransomware attack is time. Having a procedure already in place is particularly important in especially malicious ransomware attacks that involve the destruction of an organization's files or, perhaps worse, the exfiltration of especially sensitive and proprietary records.

Crowell & Moring prepares its clients for ransomware attacks with defensive strategies, corporate governance best practices, and internal and external communication outreach protocols targeted to their unique businesses and networks, as exemplified in this recent checklist that serves as a useful guide for cybersecurity incident response associated with a ransomware attack.

One of our primary tools for pre-incident preparation is the tabletop exercise. Tabletop exercises are a cost-efficient tool for testing and preparing a company's readiness. They are designed to develop "muscle memory" using realistic scenarios in a neutral, non-disruptive atmosphere for responding to a real incident under the protection of attorney-client privilege. They provide real-world, hands-on "know-how" for dealing with an incident and help executive leadership to practice communications and decision-making during the crisis.

In all cases, our experience has demonstrated how critical it is for an incident response plan to be in place and "road tested" before an incident occurs. It is simply too late to execute a response for the first time in the midst of an incident. The company must know in advance, for example:

- Who will lead the response, and who will fill other key roles in the response team;
- How will the company communicate, and what are the alternatives if telecommunications and/or e-mail are compromised; and
- How are issues escalated to leadership, on what cadence and according to which criteria?

We also assess and enhance incident response policies and procedures to provide road maps to help organizations respond properly and effectively following a ransomware attack, including compliance, crisis management, vendor management, and business continuity plans. We bring a seamless team of technical and legal professionals to the often-complex issues confronting our clients and can draw upon our firm's collective experience that cuts across multiple industries and areas of expertise. As the number of ransomware attacks continue to increase, it remains clear that preparation is key to mitigating potential risks and helping ensure an effective response in the case of 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

**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

**Matthew B. Welling**
Counsel – Washington, D.C.
Phone: +1 202.624.2588

Email: mwelling@crowell.com