Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Allaying Ransomware Threat To Private Funds Amid Pandemic

By **Brian Daly, Marc Elovitz and Edward Sadtler** (August 27, 2020, 4:14 PM EDT)

Cybercriminals are targeting businesses of all kinds with ransomware attacks. As these attacks become more sophisticated, carrying the potential to effect a wholesale inability to access a firm's entire electronic infrastructure, ransom demands have increased — often reaching eight figures.

Because these denial-of-access attacks have been so effective, making ransom payments has become mainstream in corporate America.

Private fund managers may be particularly attractive targets. Firms that are active traders could face potentially large trading losses if locked out of their systems. Firms that buy controlling stakes in companies could face ransomware attacks at both the manager and portfolio company levels.

With the recent surge in ransomware incidents, driven in part by vulnerabilities created due to the COVID-19 pandemic,[1] it is more important than ever for fund managers to take steps to safeguard their systems and data against an attack.

Recent alerts from the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations[2] and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency[3] underscore the importance of preparedness and operational resiliency in contending with the threat of ransomware attacks.

What is ransomware?

Ransomware is a type of malware designed to block an organization's access to its information systems, and/or permit unauthorized access to potentially sensitive data, until a ransom is paid. Ransomware perpetrators typically demand a ransom in exchange for returning control over the compromised systems to the organization and/or agreeing to not publicly disclose or use the data accessed.

There are numerous routes ransomware can take to access a firm's computers. Phishing scams are one of the most common delivery methods of malware used to propagate ransomware attacks. Phishing messages employ a combination of legitimate business names and domains, professional terminology and language implying urgency to deceive recipients as to the validity of the messages and to activate attachments.

What is relevant for managers in the latest ransomware attacks?

Private fund managers may be inviting targets for these attacks. Managers may be seen as financially attractive targets — deep pockets by cybercriminals seeking six- and seven-figure ransoms.

Further, the public disclosures required of managers can, in some cases, be fertile ground for the types of information cybercriminals use to prey on targets. For example, the identification of the names of senior management personnel could assist cybercriminals in identifying individuals to target.

As with other businesses, ransomware attacks can wreak havoc on fund managers in a variety of ways, some of which are more obvious than others. While attacks on administrators and other service providers who retain the fund's books and records risk compromising sensitive information stored by the vendor, ransomware attacks that include a denial-of-service component have the potential for even more disturbing consequences.

In these attacks, the cybercriminal encrypts or otherwise blocks access to a firm's information systems, rendering these systems unusable.[4] This leaves a fund manager unable to carry out basic functions.

For an active trading firm, for example, the prospect of being unable to view a portfolio or to trade or hedge positions for even a portion of a trading day could be untenable. However, all categories of fund managers should be implementing safeguards to mitigate the risk of ransomware attacks.

Of course, vendor diligence and cooperation remains an important part of the landscape. A recent attack on the vendor of a fund administrator, for example, exposed the personal information of investors for a large number of the administrator's fund clients.[5]

While, in these instances the service provider contends with the attack while it is happening, upon notification of the attack from the administrator, fund managers are left to evaluate and address the potential for legal obligations and reputational harm as a result of the attack.

How can managers increase their preparedness for a ransomware attack?

Recommendations From Regulators

The risks presented by ransomware attacks have not gone unnoticed by regulators. On July 10, OCIE released an alert[6] urging managers and other registrants to familiarize themselves with the risks of ransomware attacks and to prepare their internal systems to prevent, repel and mitigate attacks. The OCIE alert provides examples of measures to be considered and recommends that market participants monitor CISA's cybersecurity alerts.

In an Aug. 12 OCIE alert[7] focused on COVID-19 compliance risks, OCIE echoed concerns over cybersecurity attacks and provided similar guidance for maintaining effective policies and procedures.

The specific actions recommended by OCIE and CISA to bolster institutional protection against ransomware attacks include, among others, the following:

- Provide personnel with cybersecurity and resiliency training, in particular on how to identify and thwart phishing scams, creating a strong password and regularly updating it and exercising caution when using removable media.[8]

- Implement internal policies to ensure regular and automatic updates to anti-virus and anti-malware software and frequent scans for, and patches to, system vulnerabilities. This may sound simple, but the failure to keep systems current is frequently among the causes of successful ransomware attacks.

- Evaluate the firm's ability to maintain systems and restore operations in the event of an attack. This includes creating regular backups and storing them in a different geographic location, establishing perimeter security by securing the boundary between a fund's private network and public internet, and considering the feasibility of writing backup data to an immutable storage system, which does not allow data to be deleted or altered once written.

For the most current guidelines and recommendations on avoiding and protecting against a ransomware attack, fund managers should periodically review OCIE's cybersecurity webpage,[9] which contains related guidance and resources.

Insights for Institutional Preparedness

While the individual recommendations are useful criteria to analyze, the key takeaway from the OCIE and CISA guidance is that cybersecurity efforts and, in particular, steps designed to protect a manager from a ransomware attack, are as much a part of a private fund manager's compliance obligations as the need to take steps to prevent crimes such as insider trading.

Among other things, this means fund managers should:

- Assess organizational change needed to enhance preparedness for an attack. At the heart of this assessment is communication. For instance, managers should develop a specific communications plan that can be activated in the event of a breach to rapidly engage key internal and external IT, legal and other advisers. The chief compliance officer should be integrated into the cybersecurity effort and should be able to speak to the firm's efforts in that area.

- Test preparedness by conducting table-top exercises. This is a hands-on session through which personnel would be guided by IT and legal professionals through a true-to-life ransomware attack during which, at each stage, participants would discuss how the firm would respond based on existing protocols and resources. After the exercise, a remediation plan is developed based on the potential deficiencies observed.

- Review the fund's cyber insurance policies to see what is covered and address any gaps in coverage.

- Maintain situational awareness of the latest threats by understanding the data stored in the fund's system and keeping up to date on recent news and alerts regarding threats to that data's security.

Brian T. Daly, Marc E. Elovitz and Edward H. Sadtler are partners at Schulte Roth & Zabel LLP.

Schulte Roth & Zabel special counsel Kelly Koscuiszka, and associates Jennifer A. Gordon and Jaclyn N. Malmed, contributed to this article.

[1] In a recent advisory, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") identified the migration of businesses to remote access during the COVID-19 pandemic, and the resulting potential for system vulnerability, as a key reason for the substantial increase in ransomware and other cybersecurity attacks on financial institutions' remote systems. See https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf.

[2] See OCIE alert https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.

[3] See CISA alert https://us-cert.cisa.gov/ncas/alerts/aa19-339a.

[4] In a recent example reported by WIRED and other popular media, Garmin, a manufacturer of fitness-oriented devices and wearables, experienced an attack in which a cybercriminal employed a ransomware attack to encrypt Garmin's systems, resulting in a complete shutdown of user access to Garmin's systems. Garmin is believed to have paid a multimillion-dollar ransom to avoid a protracted disruption to its business. See https://www.wired.com/story/garmin-ransomware-hack-warning/.

[5] A Wall Street Journal article reporting on the breach noted that it was the latest in a string of attacks that have affected financial service companies through their vendors. See https://www.wsj.com/articles/fund-administrator-for-fortress-pimco-and-others-suffers-data-breach-through-vendor-11595857765.

[6] The OCIE alert warns about the increased sophistication of cybersecurity attacks on SEC registrants. As with recent news articles, OCIE reported that cybercriminals have been orchestrating phishing campaigns and other cybersecurity attacks designed to penetrate the networks of financial institutions (including private fund managers) to gain access to internal resources and deploy ransomware, among other objectives. See https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.

[7] See OCIE alert https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf.

[8] Fund managers should advise their employees to be aware of emails coming from seemingly legitimate sources referencing common subject and attachment titles, including "invoice," "scan," "debit note" or similar terms. The body of phishing emails may be blank or comprehensive, potentially referencing that the email has already undergone a malware or virus scan. When clicking links or opening email attachments, verify that the domain names in both the sender's email address and any included hyperlinks are spelled correctly. FinCEN's recent advisory delineates red flag indicators of COVID-19-related cyber scams https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf.

[9] See the "Cybersecurity Spotlight" webpage maintained by OCIE https://www.sec.gov/spotlight/cybersecurity.