AHERN Update

Cinthia Granados Motley is the co-chair of Sedgwick LLP's Cybersecurity and Privacy practice group. In her legal practice, Motley handles data privacy and security matters assisting clients, domestically and internationally, to implement effective information security practices, including information governance and litigation readiness. Motley was named the 2017 Corporate International Global Awards Cybersecurity Litigation Lawyer of the Year in Illinois.

Sedgwick LLP

AHERN Insurance Brokerage is one of the largest full-service insurance brokerage firms specializing in the insurance needs of law firms, with over 5,000 law firm clients.

For more information on how AHERN can assist your firm, please call (800) 282-9786 to speak with a professional.

Ransomware—A Global Wake-Up Call

By Cinthia Motley, Esq., Co-chair of Sedgwick LLP's Cybersecurity and Privacy Practice Group

Originally published in Cybersecurity Today

U.S. Regulator Warns of "Evidence" of Global Cyber Assault Occurring Inside the U.S. and Steps Your Company Should Take Against a Ransomware Attack

On Friday, May 12, 2017, Laura Wolf, Critical Infrastructure Protection Lead of the Department of Health and Human Services (HHS) issued a notification stating that:

> HHS is aware of a significant cyber security issue in the UK and other international locations affecting hospitals and healthcare information systems. ***We are also aware that there is evidence of this attack occurring inside the United States.*** We are working with our partners across government and in the private sector to develop a better understanding of the threat and to provide additional information on measures to protect your systems. We advise that you continue to exercise cyber security best practices – particularly with respect to email.

This alert comes in the heels of Friday's global ransomware attack that has spread in nearly 100 countries. The attacks are being blamed on malware called WCry, WannaCry or Wana Decryptor.

So what measures can your company take to protect itself in the event of a ransomware attack?

If a company is infected with ransomware, they face two hard choices: either pay ransom to unknown criminals or try to restore its systems, if possible. With either option a company faces risks. Thus, prevention and pre-breach planning are key, including taking the following steps:

> **Update systems and software with current patches:** Ransomware spreads easily when it encounters unpatched or outdated software. The HHS has noted that the WannaCry ransomware may be exploiting a vulnerability in Server Message Block 1.0 (SMBv1). Microsoft also just released an emergency security patch update for all its unsupported versions of Windows, including Windows XP, Vista, Windows 8, Server 2003 and 2008 Editions. In addition, keeping computer and antivirus up to date adds another layer of defense that could help stop malware.

Refresh, Review, Retrain: To protect your company from a ransomware attack properly train employees on cybersecurity. Authorized users can expose a company the most when it comes to cybersecurity risks. This includes employees who are vulnerable to social engineering and phishing attacks. Thus, train employees to identify phishing attacks and perform proper authentication of third parties before providing them with data or access to the network.

Data Access Controls: Granting users access to data and systems minimally necessary to do their jobs and closely monitoring access controls can help contain the spread of initial infections.

Implement Data Loss Prevention (DLP) and Intrusion Detection Systems: Quickly identifying potential infections with intrusion detection systems can allow a company to rapidly isolate infected servers and/or endpoints (computers), also preventing the spread of initial infections. Using data loss prevention tools companies can enforce protection policies, and administrators can secure sensitive business data and prevent illegal access to data.

Implement Regular and Offsite Data Backups: In the event of a ransomware attack, decryption keys are not always provided even when ransoms are paid. Backups stored on the same infected server are often encrypted along with the encrypted data. Thus, regular data backups that are continually tested to ensure they can be restored if needed are important to help a company recover its data, resume operations and avoid paying a ransom demand. It is equally important that backups be stored offsite.

Implement, practice and update incident response and business continuity plans: Having a tested incident response plan will help an organization quickly respond to a security incident. While many organizations have information security procedures in place, it is important that those plans and procedures be reviewed to address a potential ransomware attack. Similarly, perhaps the biggest impact of a ransomware attack is the down time an organization may face, even causing business functions to come to halt. Thus, it is critically important that companies update their business continuity plans to specifically address ransomware.

Quickly deploy incident response team and protect privilege: Quick incident response team deployment is essential when faced with a ransomware attack. This should include having legal, forensic and public relations consultants, as well as law enforcement contacts identified before a security incident occurs. Top level awareness is equally important as crisis management decisions will need to be made quickly, such as: whether the ransom demand will be paid and, if so, who should negotiate the ransom payment; how and when to notify law enforcement; as well as any internal or external communication necessary. As these decisions may greatly impact a company's business, financial and legal obligations, it is critically important that in-house or outside legal counsel be involved from the outset to advise and guide the organization, including in the retention of outside consultants. This is the best measure to help protect attorney-client privilege as company executive are forced to navigate quickly through important decisions for the organization.

In short, being proactive is often easier and less costly than a reactive approach. Cyber risks present a fast evolving landscape. Data loss through cybercrime and internal risks represent increasing business exposures. Prevention is key to mitigation in this area and a better option than facing a breach unprepared. An entity that knows those risks and controls the data that flows within and outside its walls can best remain competitive in their marketplace. Using this knowledge a company can most efficiently protect sensitive data and quickly respond to security incidents.