Bryan Cave’s Jena Valdetero offers tips on cybersecurity and the COVID-19 pandemic

By Mark S. Nelson, J.D.

Jena M. Valdetero, a partner and co-leader of Bryan Cave Leighton Paisner LLP’s Data Privacy and Security Team and leader of the firm’s Data Breach Response Team, suggested a few things companies can do to help address the potential for cybersecurity breaches during the COVID-19 pandemic. Valdetero’s practice includes advising companies on a variety of data privacy and security issues, including the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Gramm Leach Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA). Valdetero also consults on transactional matters such as mergers and acquisitions that raise data privacy and security issues.

Although all companies should have cybersecurity incidence response plans, companies in some industries, such as the securities industry, also must comply with specific federal, state, or foreign regulations. Stock exchanges in the U.S., for example, must satisfy the requirements of the SEC’s Regulation Systems Compliance and Integrity (Regulation SCI).

Valdetero spoke to Wolters Kluwer about some practical tips for all types of companies that may face cybersecurity issues regarding the COVID-19 pandemic. She also noted some best practices for securities firms.

What are the cybersecurity risks to companies of more of their employees suddenly working from home?

The primary risk is people themselves. Employees who are not used to working from home may not be mindful of good WFH hygiene, including using secure wifi and secure devices. In addition, we are seeing an increase in phishing emails designed to trick employees into disclosing their user credentials and/or sending sensitive personal and financial information to a threat actor. Companies need to be realistic about human behavior and deploy measures to “save people from themselves.” Companies can help mitigate these risks by providing company-issued devices that are configured to meet the company’s data security standards, requiring multi-factor authentication at log-in, and training/reminding employees to be especially vigilant right now against cyber threats. Now also might be the time to consider turning off the email feature that displays the sender’s name, but hides the sender’s email address. We are seeing an uptick in spoofing emails (i.e., emails that appear to be from “Joan Smith” but the email address isn’t your email) and this feature helps the threat actor avoid detection. I would also increase logging, if possible. Logs are like breadcrumbs that show where
an individual went once they are inside your environment. If you have a breach, logs will be key to being able to identify what data was – and wasn’t – accessed. Companies should consider increasing monitoring, particularly since people will now be logging in from far more IP addresses than normal due to remote working.

What are some of the key issues an incident response plan should address regarding a pandemic?

As simple as it may sound, companies should make sure their incident response team members have a copy of the incident response plan, including, a list of the incident response team members and their contact information, plus back-up employees in case one of the team members is ill or unavailable. They should have a list of third parties they could call in the event of a security incident, including outside breach counsel, forensic investigators, and cyber insurers. If there are notification requirements that the company would need to meet in the event of a breach, those should be in the policy. In some jurisdictions – e.g., the EU under the GDPR or for financial institutions under NY DFS – there's a 72 hour notification requirement to the regulators. If the company is holding data on behalf of another company, your obligation is generally to notify those business partners immediately.

How can companies leverage their cyber insurance policies regarding a pandemic-related cyber breach?

Pull a copy of your policy so you have it even if you don’t have access to your computer system or email. Review your self-insured retention (i.e., the amount the company has to pay before the insurance kicks in) and make sure you have that amount in reserves. Look at your limits and make sure you are comfortable that those would adequately cover you in the event of an incident. You should understand if your policy requires you to use insurance-approved providers. Many of them do. If you want to use a breach response vendor that’s not on the insurer’s panel, you can request approval before an incident occurs. Most insurance companies are reasonable about granting such requests.

What are some of the cybersecurity risks for stock exchanges and other trading platforms that have switched to electronic-only trading in order to enforce social distancing?

Stock exchanges will always be targets of cyber-attacks because of ability to manipulate the markets if successful. This is an industry that is already very highly regulated, and likely most trading companies already have in place stringent security measures to protect against attacks, even if their employees are working remotely. If they don’t, companies should consider whether the risk of a cyber-attack is worth the need to continue to do business.