THE JOURNAL RECORD

Gavel to Gavel: Cybersecurity and the law – 2021 in review

By: Susan Lindberg Guest Columnist December 15, 2021 0

Susan Lindberg

2021 started with a bang. Hundreds of companies and government agencies reeled from the attack on SolarWinds. When the attack was discovered in December 2020, malware embedded in the software provider's code had already caused widespread security compromise to SolarWinds's customers.

In March, a ransomware attack on the U.S.' most important fuel pipeline disrupted gasoline supply, affecting prices along the East Coast. The attacks were attributed to nation-states and international organized crime groups.

Meanwhile, some employees returned to the office, but many continued to work remotely, presenting an ongoing challenge to business cybersecurity. And, with big tech under continued media and government scrutiny, consumers grew ever more aware of the collection, use, and potential breach of their personal data.

During 2021, lawmakers responded in several ways:

1. Executive order – In May, President Biden issued an Executive Order on Improving the Nation's Cybersecurity. The EO emphasizes the need for government to partner with the private sector on security. It then mostly focused on improving federal government cybersecurity. Notably, it ordered the Department of Homeland Security to create a Cyber Safety Review Board.

2. Industry-specific regulations – **a.** The Transportation Security Administration used its emergency authority to issue prescriptive requirements for owners of critical pipeline infrastructure. **b.** The U.S. Department of Defense continued to refine its new requirements for Cybersecurity Maturity Model Certification for companies that wish to contract with the DoD.

3. Enhanced data protection laws – several states, including Virginia, California, and Colorado, expanded their data privacy and notification laws to broaden the categories of information protected and types of protections required, and to accelerate required notice to customers of data breaches.

4. Expansion of foreign sanctions – the U.S. Department of Treasury Office of Foreign Asset Control continues to add to its list of parties with whom business dealings are prohibited. In 2021, this included a virtual currency exchange known for its significant involvement with ransomware actors.

What should you do?

If you collect personal data, keep up to date on the relevant privacy laws, as this area is evolving rapidly, and train your employees accordingly. For government contracts, watch the CMMC requirements closely and plan ahead. Finally, if you are the victim of a cyberattack or threatened attack, report the attack to law enforcement authorities and consider collaborating with government on prevention and response. Confidential treatment of your information and other legal protections may be available, depending on the situation. And most importantly, include legal counsel on your data privacy and cybersecurity compliance and response team.

Susan Lindberg is an attorney and shareholder in the Tulsa office of GableGotwals.