Los Angeles & Orange County
BUSINESS of LAW
Trends. Updates. Visionaries.
AUGUST 2021

Herd Immunity Can Strengthen Cybersecurity

To some people ransomware and cyberattacks – not unlike COVID-19 – strike randomly and the only thing one can do is hope that your operations are not hit. The recent mass cyberattacks on the nation's supply chain struck both large and small businesses. The SolarWinds attack compromised 100 private companies and 9 federal agencies; Colonial Pipeline's ransomware hack affected 45% of the East Coast's fuel supply; the JBS attack almost shut down the country's meat supply chain; and the Kaseya hack affected between 800 and 1,500 small businesses. Malicious emails, which are often the tip of the ransomware spear, are up 600% and the average ransom demand increased 4,000% in the last several years.

An Interconnected Web of Businesses

As these cyberattacks demonstrate, for good or bad, all businesses are connected. Cyber risk is not some other person's problem. It falls to every business to do what it can to fend off cyberattacks. Measures can be taken to protect business operations from cyber criminals. President Biden's recent cybersecurity executive order[1] uses the purchasing power of the federal government to institute such cybersecurity measures. Government contracts must now flow down privacy and security provisions to multiple supplier tiers. The entire government supply chain must contractually shake hands on privacy and security to protect sensitive data assets of the business and to fend off malware. Reasonable administrative, technical, and physical security measures and contract provisions, such as independent third-party certifications of a company's and its suppliers' cyber readiness, immunize the most personal and sensitive data entrusted to those business partners. They act like cybersecurity vaccines; if enough businesses sign up for them, the whole herd will be protected from cyber risk. The bad guys search out and capitalize on weak links in this cyber chain. If each business takes personal responsibility to protect the sensitive data to which it has access, the entire supply chain will be hardened.

Inoculating Against Cyber Risk

Summarized below are some practical measures to protect your most critical data assets.

- We can't protect what we don't know – inventory your business to identify your critical data assets.
- Take advantage of the federal government's recently launched cybersecurity ransomware resources, including a valuable website with guidance and free assessment/awareness tools – *stopransomware.gov*.
- Understand with whom your data is shared and if third parties are doing their part to protect it. Many data breaches involve small third parties not subject to a company's cyber scrutiny. Don't take exposure risks with third parties who have not demonstrated their ability to protect important data assets to which they have access.
- Build in contractual protections with all vendors for cyber risk and do annual checks to ensure that your business partners are doing what they promised on privacy and security. Enforce those privacy and security provisions and terminate business relationships where the third party has failed in its obligations.
- Appoint a manager accountable for cybersecurity to report regularly to executives.
- Have separate backup and recovery measures in place so business operations can continue even in a ransomware attack.
- Do the work to avoid being a soft target and vaccinate your business against cyber risk. Have multifactor authentication to counter phishing. Educate your workforce and suppliers on proper digital hygiene.

Together the business community can achieve cybersecurity herd immunity.

Sharon R. Klein is a partner at Blank Rome LLP and chair of the firm's Privacy, Security & Data Protection Practice Group, focusing her practice on data privacy, cybersecurity, and complex technology transactions. She can be reached at sharon.klein@blankrome.com.

[1]Executive Order on Improving the Nation's Cybersecurity, *whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity*

This content is produced by the L.A. Times B2B Publishing team. It doesn't involve the editorial staff of the L.A. Times.

Recap of In-House Counsel Leadership Awards