Executive order addresses cybersecurity

By Natalie M. McMahan

This article appeared as a Guest Column in The Journal Record on June 23, 2021.

Cybercriminals have held a number of industries hostage in recent months, and otherwise exploited companies' vulnerabilities to profit directly from the stolen data. Most notably, ransomware attacks shut down meat producer JBS and the Colonial Pipeline. Other recent data breaches affected McDonald's, Volkswagen, and approximately 100 companies using SolarWinds. Last month, the city of Tulsa suffered its own shutdown caused by a ransomware attack.

Natalie M. McMahan

On May 12, the president issued an executive order outlining the administration's plans to address "malicious cyber campaigns that threaten" both the public and private sectors. The Biden administration also created a new cybersecurity role on the National Security Council; Deputy National Security Advisor Anne Neuberger recently met with the National Association of Attorneys General to discuss the administration's ransomware strategy. She has also engaged business leaders to work with the federal government in its

efforts to elevate cybersecurity issues.

The cybersecurity executive order matters because it will push industry and those that do business with the federal government to implement heightened security protocols.

Here are some key takeaways from the executive order that may be aspirational but will certainly be influential:

- Removing barriers to sharing threat information.
- Modernizing cybersecurity, including the adoption of best practices.
- Enhancing software supply chain security.
- Establishing a cyber safety review board (similar to the National Transportation Safety Board).
- Standardizing the government's response to cybersecurity vulnerabilities and incidents.
- Improving monitoring operations and alerts to identify and respond to cyber incidents.

If this order does not impact your business directly, it will certainly impact the commercial-off-the-shelf (COTS) software that your company uses, as the government is likely a user of the same product. In terms of cybersecurity, this is good news.

While all 50 states have passed legislation requiring notifying individuals in the event of a data breach that discloses their personal information, additional data privacy regulations primarily exist at the federal level and only apply to certain highly regulated industries, i.e. health and financial information. Several states have passed consumer data privacy laws that regulate how businesses collect data from customers. However, in the most recent legislative session, Oklahoma did not pass expanded privacy protections for customers.

Cybersecurity measures, outside of making required notifications in the event of a data breach, are not mandated

by Oklahoma law or the Biden administration's new executive order. However, the most compelling reason to implement and maintain cybersecurity measures is money. Breaches are expensive, consuming time and resources to remedy. The adage holds true that an ounce of prevention is worth a pound of cure.

Creating an information assurance plan for your business requires critically thinking about the confidentiality, integrity, and availability of both your network and the data stored on it for employees accessing from their workspace, or, as many of us have over the past year, from home.

Attorney Natalie M. McMahan is a litigation attorney who represents individuals and both privately-held and public companies in a wide range of civil litigation matters.

***For more information on how the information in this article may impact your business, please call 405.552.2437 or email* Natalie M. McMahan.**

*Follow our coverage on **FACEBOOK***