How will the executive order on cybersecurity impact businesses?

Summary of the order

On May 12, 2021, President Joseph Biden issued a sweeping executive order to improve the nation's cybersecurity.

The order comes in the midst of a series of high-profile incidents, such as the ransomware attack that shut down Colonial Pipeline operations and the Solar Winds hack that impacted both U.S. agencies and private companies such as Intel and Microsoft.

While the order focuses on the federal government, organizations in the private sector will also be affected as new standards and stricter regulations are implemented. Many of these are already recommended as best practices for any business—for example, using encryption to secure data, and adopting a zero-trust framework requiring all users to be authenticated and authorized.

"We encourage private sector companies to follow the federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents," the order states.

Provisions in the executive order include:

- Implementing stronger cybersecurity standards in the federal government, including the adoption of a zero-trust security model and use of encryption and two-factor authentication.
- Improving security of the software supply chain by establishing baseline security standards, including requiring developers to offer greater transparency and make data publicly available.
- Establishing a Cybersecurity Safety Review Board, modeled after the National Transportation Safety Board, to analyze cyber incidents and make concrete recommendations for improving cybersecurity.
- Improving detection of malicious activity on government networks via Endpoint Detection and Response (EDR) tools.
- Removing barriers to threat information sharing between government and the private sector.