Armstrong Teasdale

June 11, 2021 • Advisory • www.atllp.com

BIDEN ADMINISTRATION BESEECHES BUSINESS LEADERS – BETTER CYBERSECURITY NOW

Last week, after weeks and months of advisories and admonitions relating to recent ransomware attacks, the White House issued an extraordinary letter to "Corporate Executives and Business Leaders" urging them:

To understand your risk, ***immediately convene their leadership teams to discuss the ransomware threat and review the corporate security posture*** and business continuity plans to ensure you have the ability to continue or quickly restore operations.

(Emphasis added).

The letter also stated that the private sector has a critical responsibility to protect against threats and to "ensure [the] corporate cyber defenses match the threat." Referring back to the recent *Executive Order on Improving the Nation's Cybersecurity*, the letter strongly urged business leaders to implement these "high impact" best practices:

- *Multifactor authentication* – because passwords alone are routinely compromised.
- *Endpoint Detection and Response* – to support proactive detection of cybersecurity incidents.
- *Encryption* – for data at rest and in transit, so if data is stolen it is unusable.
- A skilled, empowered security team to share and analyze threat information.
- A security team to administer an effective patch management program.

That the letter was specifically directed at business leaders is not unusual. Federal agencies have repeatedly urged business leaders that adherence to cybersecurity 'industry standards' is a legal obligation.

In July 2019, the Federal Trade Commission (FTC) announced a $700 million settlement with Equifax for deficient cybersecurity practices. As part of the settlement, the FTC mandated that Equifax's directors and officers:

PEOPLE

Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

White-Collar Criminal Defense and Government Investigations

Internal Investigations and Regulatory Compliance

- be informed about any material evaluations or updates to its information security program every 12 months;
- evaluate, assess and identify gaps and weaknesses in Equifax's information security program; and
- certify every year for 20 years that Equifax is in compliance with the FTC's settlement.

In January 2020, the FTC announced that it would be implementing a "new and improved" approach to cybersecurity enforcement actions that requires "Board[s] or similar governing bodies" and "senior managers" to "gather detailed information about the company's information security program, so they can personally corroborate compliance" with the organization's written information security program (WISP).

Based on research that suggested the FTC's efforts to improve corporate governance on cybersecurity issues was timely and well founded, the FTC stated that it would create further incentives for high-level oversight of, and appropriate attention to, cybersecurity.

In April 2021, the FTC issued detailed guidance on the role business leaders must play in cybersecurity. In a post titled *Corporate boards: Don't underestimate your role in data security oversight*, the FTC stated that "[c]ontrary to popular belief, data security begins with the Board of Directors, not the IT Department."

The FTC then listed strategies that business leaders should consider implementing which included:

- *Build a team of stakeholders from across your organization* – the team "should incorporate stakeholders from business, legal, and technology departments across the company – both high-level executives and operational experts."
- *Establish board-level oversight* – this helps to "ensure that cybersecurity threats, defenses, and responses have the attention of those at upper echelons and get the resources needed to do the job right."
- *Hold regular security briefings* – cybersecurity is dynamic, therefore, "[r]egular briefings prepare boards to carry out their oversight responsibility, navigate the security landscape, and prioritize threats to the company."

In addition to the letter, the White House issued a memorandum that requires federal prosecutors involved with ransomware or digital extortion investigations to:

- utilize enhanced notification requirements to relevant federal taskforces of findings and developments; and

- coordinate with federal agencies and taskforces, including with the Department of Justice's Criminal Division's Computer Crime and Intellectual Property Section (CCIPS).

Despite the United States Supreme Court's ruling last week limiting certain aspects of the federal government's authority to prosecute cybersecurity incidents, the letter, recent FTC guidance, and the memorandum demonstrate the central role of the federal government and business leaders in preventing and investigating cybersecurity attacks.

If you have any questions about your organization's or your Board's cybersecurity legal obligations, please contact any of the authors of this advisory or your regular Armstrong Teasdale attorney.