CARLTON FIELDS

Biden Administration Issues Practical Guidance for Ransomware Attacks

CYBERSECURITY AND PRIVACY | TECHNOLOGY | TECHNOLOGY & TELECOMMUNICATIONS | JUNE 15, 2021


Joseph W. Swanson


John E. Clabby


Christina M. Gagnier


Michael L. Yaeger


Patricia M. Carreiro

On June 2, 2021, President Biden issued a memorandum providing "recommended best practices" for protecting against ransomware. The memorandum urged corporate executives and business leaders to:

1. Adopt the "best practices" laid out in President Biden's May 12 cybersecurity executive order. This May executive order applied to the government itself and to select federal contractors, and laid out requirements and best practices that include multifactor authentication, encryption, endpoint detection and response, logging, and operating in a zero-trust environment.
2. Create backups of data, system images, and configurations, regularly test them, and keep the backups offline.
3. Update and patch systems promptly.
4. Test incident response plans.
5. Use a third-party penetration tester to test system security and the organization's ability to defend against a sophisticated attack.
6. Segment networks, limit internet access to operational networks, and regularly test contingency plans.

These are practical, high-level tips, and leave many questions for companies to answer in examining their cybersecurity posture. How broadly should encryption be used? How much logging should be done? How often should backup data be synched, backups tested, and incident response plans rehearsed? How often should third-party tests be done, and how extensive should they be? How segmented must networks be? The answers require the same risk-based approach already in use by most top companies.

But the president's June 2 memorandum is noteworthy for at least two reasons beyond the substantive advice. First, the memorandum's direct appeal to the private sector illustrates not only the importance of addressing ransomware but also the hands-on approach this administration intends to take with cybersecurity matters. With high-profile ransomware attacks recently grabbing headlines across the nation, cybersecurity generally - and ransomware in particular - has become an issue of general concern for the American public. This memorandum only underscores that point.

Second, regulators and litigants may point to the memorandum to argue that it sets forth a standard of care that organizations must adhere to when it comes to cybersecurity. The efficacy of that argument will depend on any given matter and its unique facts, but given the increasing frequency of government investigations and/or litigation in the wake of a cyberattack, organizations should consider the possibility that an adversary will scrutinize their security posture relative to this memorandum.

So what should organizations do to guard against cyberattacks generally and ransomware in particular? In light of the White House's memorandum, it is especially worthwhile to:

1. Reconsider the extent of your, and your vendors', use of multifactor authentication, encryption, endpoint detection and response, logging, and network segmentation.
2. Double-check and test your backups, including the extent to which those backups are maintained offline.
3. Verify your patch maintenance.
4. Ensure your incident response plan is up to date, and then undertake a tabletop exercise to test that plan in practice.
5. Work with a third-party cybersecurity expert to audit your system, involving outside counsel to maximize the application of the attorney-client privilege and work product doctrine.

6. Based on any findings from that audit, evaluate the extent to which those findings should be addressed and in what priority.
7. Throughout this prophylactic work, document the steps you have taken, your considerations, and your bases for any decisions made. This record could serve you well in future breach litigation or an enforcement proceeding.