CARTER/LEDYARD

our resources

Cybersecurity: Respond to the Rising Threat of Hacking

May 17, 2021

The threat of cyber hacking just keeps getting worse. Since the beginning of this year, the hack of Microsoft Exchange Servers that began in January gave hackers access to user emails and passwords on over 250,000 servers belonging to over 30,000 organizations in the U.S. Weeks earlier, it was discovered that in 2020 hackers in Russia had planted malware on Orion software used by SolarWind to manage IT resources, and this malware was distributed in software updates to over 33,000 SolarWind customers. A few days ago it was disclosed that Colonial Pipeline had been hacked in an extortion attempt that shut down one of the largest gas pipelines in the U.S.

In response to the recent Colonial Pipeline hack, President Biden issued an Executive Order on May 12[1] to increase cyber security at federal agencies and to require government contractors to step up their cybersecurity game. The Executive Order will have direct and indirect benefits for the private sector.

The Colonial Pipeline Hack. In early May a Russian hacker gang calling itself "DarkSide" inserted malware that froze the operating systems of Colonial Pipeline; the hackers demanded a very large ransom in Bitcoin to disable the malware. It's been reported that Colonial paid a ransom of almost $5 million in order to keep its critical service working, but the hackers' software repair tool didn't work well and Colonial's pipeline service was disrupted for days, resulting in shortages, panic buying and gas hording at the pump, and significant price rises for customers along the route of the Colonial pipeline between Houston and New York City.

After days of frantic activity by Colonial, software security firms and government experts, Colonial resumed operations, though with huge damage to its reputation and loss of confidence among retail consumers.

Several hacker groups have disappeared from the web in the last few days but it is expected that they will reappear, Whack-a-Mole style. It's likely that the DarkSide gang will find other targets for their "service as a hire" extortion efforts soon enough.

The May 12 Executive Order. On May 12 President Biden issued an Executive Order to improve cyber security at federal government agencies and at the private companies that supply software and other cyber services under contract. These steps include:

- Increasing the sharing of information about cyber threats and risks amongst service providers and federal agencies in order to accelerate incident deterrence, prevention, and response efforts.

- Standardizing procurement contract language across federal agencies to require service providers to keep records in a standardized format about cyber events, detection and responses to those events, and investigation thereof, to require providers to share that information, and to require that providers collaborate with each other and with federal agencies in cyber breach cases.

- Requiring federal agencies to adopt several security measures including using cloud technology to prevent, detect and assess and remediate cybersecurity incidents, multifactor authentication, and encryption to protect data at rest or during transmission.

- Requiring federal agencies to evaluate the security practices of software and IT service providers, and requiring service providers to attest to compliance with cybersecurity best practices. Federal use of software and services that don't conform will be discontinued.

- Standardizing the federal government's playbook for responding to cybersecurity risks and incidents while also allowing for necessary flexibility to deal with different incidents as they arise.

- Requiring standardized logging of cyber incidents, with rules governing encryption and retention of logs.

- Maximizing early detection of cybersecurity vulnerabilities and incidents on federal agency networks.

- Establishing a Cyber Safety Review Board, comprised of federal officials and representatives from private-sector entities.

There is no statutory power for the federal government to mandate cybersecurity reforms in the private sector. However, the Executive Order mandates several steps that will improve private sector security directly or indirectly:

- The National Institute of Standards and Technology ("NIST") is directed to advise the public about the security of Internet of Things (IoT) devices including labelling requirements dealing with security.

- NIST will publish security ratings for commercially available software.

- Several agencies will collaborate to develop a playbook for cyber incident response.

- Some of the improvements mandated for government agencies probably will be adopted as best practices in the private sector, such as the "seal of approval" that agencies will grant to software and IT services that are accepted for government procurement, and standards for incident logging and response. Insurance companies may consider whether customers adopted those steps before honoring claims for hacking incidents.

What should private business be doing to respond to this heightened threat environment?

- Review cybersecurity process and procedures in-house and with security experts. This review should include consideration of the steps that the Executive Order addresses: multifactor authentication, protocols for access to data, using cloud technology as a security tool, encryption, and a comprehensive review of cyber security safeguards and procedures, including installation of all software upgrades and patches and reviews of cybersecurity practices of service providers.

- Review cybersecurity insurance coverage. It's likely that carriers will tighten their coverage requirements as claims increase.

- Employee training. Employees and service providers are often the weakest link in cybersecurity, inadvertently granting access to bad actors who are phishing and spoofing. Personnel training should be refreshed on an urgent basis.

---

[1] Executive Office of the President, Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021.

---

related professionals

H. Thomas Davis, Jr. / Partner
D 212-238-8850
davis@clm.com

John M. Griem, Jr. / Partner
D 212-238-8659
griem@clm.com

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com