wiley

ARTICLE

How Gov't Cyber Efforts Will Affect Companies This Year

Law360
January 3, 2018

December 2017 saw a flurry of federal cybersecurity activity, following several major attacks and the attribution of the WannaCry malware to North Korea. We expect a busy 2018. President Donald Trump's national security strategy and executive orders were heavy on cyber and the private sector. Policymakers are considering how to secure the internet of things. The National Institute of Standards and Technology is revising its "Framework for Improving Critical Infrastructure Cybersecurity."[1] The U.S. Department of Homeland Security plans an aggressive approach to public-private collaboration and Congress has several bills in play. Here, we offer eight predictions about how federal cyber activities will affect the private sector in the year ahead.

1. Expectations Will Rise for Corporate Governance and Accountability, As Reflected in the National Security Strategy and Executive Orders

The president addressed cybersecurity several times. His national security strategy promised to increase the United States' offensive capabilities and called out hostile nations,[2] but it also previewed more demands on the private sector, from infrastructure owners to communications networks. A "priority action" states: "[T]he U.S. Government will work with the private sector" to address "bad activities at the network level" because "[m]alicious activity must be defeated within a network and not be passed on to its destination whenever possible."[3] As Tom Bossert, assistant to the president for homeland security and counterterrorism, said, "the President calls today, on the private sector to increase its accountability in the cyber

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

realm"[4] and help the government. Such "accountability" will mean more work for the private sector.

In May 2017, Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," set in motion numerous reports that come due in 2018. One involves increasing market transparency related to cybersecurity risk.[5] What to expect? Potentially more robust U.S. Securities and Exchange Commission disclosures and scrutiny of corporate governance as it relates to cyber.[6] We have not yet seen the business judgment rule tested in litigation over companies' cyber decisions, but prudent companies are taking a more active approach. Regulators will take note.

2. The Department of Homeland Security Will Be More Assertive

In late 2017, we saw the confirmation of a new secretary of DHS with a strong interest in cyber. A series of comments from federal leaders called for more muscular work by DHS with the private sector. DHS wants "to drive the market toward more secure, scalable, and interoperable solutions."[7]

DHS Assistant Secretary for the Office of Cybersecurity and Communications Jeanette Manfra stated "we see some gaps between what an entity might consider adequate security for themselves or their sector and what is in the public's interest."[8] Noting that many "critical services and functions ... are run by the private sector," she called for increased "public-private collaboration [that] is entirely voluntary and provides companies with strong liability and privacy protections should they participate."[9]

But Assistant Secretary Manfra hinted that the status quo is not where it should be, noting that "[t]o ensure adequate security in the private sector, DHS plans to move beyond only offering voluntary assistance to more proactively becoming the world leader in cyber risk analysis and intervening directly with companies when necessary."[10] It is unclear what such intervention will look like, but in other settings DHS has noted its limited authorities, and it may put additional pressure on the private sector.

3. NIST Will Impact the Private Sector on a Range of Topics

Nearly every discussion of cyber includes a reference to NIST, which is nestled in the U.S. Department of Commerce. As a nonregulatory body that understands technology and advises the government, NIST is increasingly providing guidance on cybersecurity. It is poised to influence private activity in many areas, from the IoT to "bug bounty" programs.

Its flagship cyber document is under revision now, with innovative changes that companies will need to consider, including endorsement of "vulnerability disclosure programs" and more robust information-sharing. NIST has laid out an aggressive action plan for 2018, much of which could be quite productive if it focuses its efforts. Some of NIST's privacy initiatives, which have roots in requirements for federal agencies, wander off its core mission and could detract from other important work. NIST can really help drive cybersecurity for the private sector by focusing on small business uses of the framework and international engagement to promote

it.

NIST has underway many other activities affecting cyber. It often flies below the radar but can be influential. Developing technical standards for everything from online authentication to encryption to risk management, NIST's expectations are rising, and its standards are adopted across the government and among private entities. The private sector should watch those efforts and engage where needed.

4. Procurement Demands Will Raise Stakes and Have Effects Across the Economy

The federal government must do a better job securing its networks and sensitive information. The president's national security strategy says, "Federal networks also face threats. ... The government must do a better job of protecting data to safeguard information and the privacy of the American people."[11] That is an understatement, considering recent U.S. Office of Personnel Management and SEC breaches and reports faulting agency cyber management.[12] It is an enormous challenge that is likely to be addressed piecemeal in 2018.

For example, the National Defense Authorization Act addresses federal security. Among other things, it establishes a Technology Modernization Fund and Board designed to improve and replace existing federal information technology and cybersecurity systems through acquisitions.[13] Notably, the NDAA identifies products and services it prohibits the government from acquiring. Certain U.S. Department of Defense systems must not include telecommunications equipment or services produced by Huawei, ZTE, or any company owned, controlled by, or otherwise connected to the Chinese or Russian government.[14] Not surprisingly, contractors will come under increased pressure as they start to comply in 2018 with the requirements in DFARS 252.204-7012 and NIST Special Publication 800-171 governing the protection of certain government information. Contractors can expect increased obligations and scrutiny.

These are just a few ways the government may push ahead on cyber. As explained below, Congress is looking at federal agencies and proposals that could affect companies doing business with the government.

5. Congress is Itching to Do Something, Heightening Oversight Concerns

2017 saw numerous hearings on multiple aspects of cyber, from mobile security to cyberthreat information sharing. Not to mention many hearings related to the Equifax breach. Multiple bills have been introduced in Congress that could affect private companies' cyber posture.[15]

Several congressional committees have jurisdiction touching cybersecurity: the Senate Committee on Homeland Security and Governmental Affairs; Senate Committee on Commerce, Science, and Transportation; House Committee on Oversight and Government Reform; House Energy and Commerce Committee; and the House and Senate Judiciary Committees, to name just a few. Even the Small Business Committee is engaged, introducing legislation to foster cyber information sharing with DHS. One major bill would reorganize DHS'

cyber activities, and another would authorize so-called "active cyber defense" which some consider a variant of "hacking back," which is fraught with complexity.

From numerous data security and breach notification bills following the Equifax breach, to new standards and obligations on those selling IoT devices to the government, Congress is poised to act. At a minimum, expect Congress to continue being reactive to the news cycle, focusing on vulnerabilities and incidents as they occur.

6. National Security Review of Global Deals and Equipment Use Will Increase

The president has indicated that "this Administration will work with the Congress to strengthen the Committee on Foreign Investment in the United States to ensure it addresses current and future national security risks."[16] This committee scrutinizes deals involving countries seen as security threats and there are several proposals in play to make its role even more impactful. In the meantime, look for enforcement and oversight from the U.S. Department of Justice, the Department of Treasury, DHS and others as they grapple with numerous "mitigation agreements" from CFIUS and the "Team Telecom" group that oversees compliance with network security agreements with communications companies. The Foreign Investment Review Staff of DOJ's National Security Division has broad reach and visibility. With new leadership at NSD expected soon, companies may find themselves on the receiving end of more oversight about cyber, in the form of site visits, requests for documents, and government suggestions about technical and equipment security.

Agencies will be aggressive in reinforcing federal priorities related to supply chain security, cyber vulnerabilities and hostile nation state access. Supply chain integrity features prominently as well in the recent NDAA restrictions on DOD equipment from Huawei and Kaspersky Lab, as well as DHS' decision to bar the use of Kaspersky in federal systems. As we saw in late 2017 when the DOJ reached a resolution with Netcracker Technology Corp., part of Japanese technology company NEC Corp. The nonprosecution agreement will require improved security protocols for software to resolve a criminal investigation claiming that its contracted work created security "degradation" at the Defense Information Systems Agency. Where needed, the DOJ can flex its muscle.

7. International Regulation Will Challenge Companies and Threaten U.S. Technology Dominance

From the IoT to data security and privacy, other countries are not standing by. There are multiple activities underway to set standards and increase regulation across the globe. From the EU's directive on security of network and information systems (NIS Directive)[17] to Chinese cybersecurity law, many countries are passing laws that amount to forced data localization and promise to complicate international trade.

On the upside, some countries are cooperating to share information and collaborate on global enforcement. Multinational companies should support such efforts as expectations mount for increased work to defeat bad actors. A good example is Microsoft and Facebook's recent efforts to address cyberattacks. The companies "helped disrupt [distribution of malware], cleaned customers' infected computers, disabled accounts being

used to pursue cyberattacks and strengthened Windows defenses to prevent reinfection."[18] We are likely to see governments increasingly expect this sort of cooperation as part of being a "good corporate citizen." Companies will need to consider how they approach cooperation among private companies and with the government, given global sensitivities in a post-Snowden world.

Hopefully the United States government will champion American values of openness, transparency, and free markets abroad to ensure a level playing field for our innovators and companies.

8. Multistakeholder Efforts Will Be Important to Stave Off Regulation

The private sector has long resisted prescriptive regulation, because collaborative private sector-led activities generate flexible best practices that are preferable to static regulation. From collaborative work by the National Telecommunications and Information Administration on IoT patching and soon on software security assurance and bills of materials, to information sharing in information sharing and analysis organizations and information sharing and analysis centers, collaboration has been the model for addressing security.

We expect this to be a theme of a coming government report on botnets and distributed denial-of-service attacks.[19] The Commerce Department's National Telecommunications and Information Administration is expected to release it on Jan. 5. The NTIA has been told that no one actor can "solve" the problem,[20] so look for the NTIA to call for use of existing tools, more education, better endpoint (i.e., device) security, updates and patching, and more engagement internationally.

This public-private collaborative model has been persuasive to policymakers, but there is a growing desire for efforts to show results. Policymakers expect even more engagement by the private sector, and are starting to "nudge" companies toward more tangible results. NIST, for example, will be looking at measurements and metrics for private cybersecurity risk management. If the private sector wants to avoid ill-advised mandates and approaches from regulators, it should help inform that initiative and others.

Conclusion

2018 will be a busy year for cyber. Even without direct regulation, the private sector will be affected, given its control of infrastructure and technology and increasing government concern about networks, supply chain security, software, IoT, patching, and technical integrity across the economy. Executive boards will be expected to ratchet up their review of internal risk management, and companies will face demands to share information and expertise with the government. Overall, these enhanced government expectations for private sector collaboration will raise the stakes for private companies.

To view a PDF of the article, click here.

[1] See NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 Draft 2 (Dec. 5, 2017), https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

[2] See President Donald J. Trump, National Security Strategy of the United States of America (Dec. 2017), ("2017 National Security Strategy"), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[3] Id at 13.

[4] Thomas Bossert, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017), https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

[5] See Exec. Order No. 13800, Strengthening the Cybersecurity of Federal networks and Critical Infrastructure, 82 Fed. Reg. 22391 (May 11, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

[6] See, e.g., Securities and Exchange Commission Chairman Jay Clayton, Statement on Cybersecurity (Sept. 20, 2017) ("The Commission also will continue to evaluate th[e 2011 Cyber Risk Disclosure G]uidance in light of the cybersecurity environment and its impacts on issuers and the capital markets generally."), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20#_ftn.

[7] Jeanette Manfra, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017), https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

[8] Id.

[9] Id.

[10] Id.

[11] See 2017 National Security Strategy at 12-13.

[12] See U.S. Office of Personnel Management, Cybersecurity Resource Center: Cybersecurity Incidents, https://www.opm.gov/cybersecurity/cybersecurity-incidents/; U.S. Securities and Exchange Commission Chairman Jay Clayton, Statement on Cybersecurity (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20. See CYBERSECURITY: Actions Needed to Strengthen U.S. Capabilities, GAO-17-440T (Feb. 14, 2017), https://www.gao.gov/products/GAO-17-440T

[13] See National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91 (2017).

[14] See id.

[15] See, e.g., Consumer Privacy Protection Act of 2017, S.2124; Cyber Shield Act of 2017, S.2020, and companion bill H.R. 4163; and Consumer Data Protection Act, S.2188 and companion bill H.R.4544.

[16] See 2017 National Security Strategy at 22.

[17] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[18] Microsoft, Microsoft and Facebook Disrupt ZINC Malware Attack to Protect Customers and the Internet From Ongoing Threats (Dec. 12, 2017), https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/.

[19] See Exec. Order No. 13800, Strengthening the Cybersecurity of Federal networks and Critical Infrastructure, 82 Fed. Reg. 22391 (May 11, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

[20] See NTIA, report on Responses to NTIA's Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats (Sept. 18, 2017), https://www.ntia.doc.gov/files/ntia/publications/rfc_comment_summary_20170918.pdf.