The Heritage Foundation

ISSUE BRIEF

No. 6081 | MAY 26, 2021

EDWIN MEESE III CENTER FOR LEGAL AND JUDICIAL STUDIES

Time for a National Cyber Incident Disclosure Requirement

Michael Ellis

KEY TAKEAWAYS

Recent cyberattacks on American companies demonstrates critical weaknesses in U.S. cybersecurity defense.

Federal legislation that requires and incentivizes companies to disclose hacks would improve U.S. cybersecurity by enabling the government to help in time.

Effectively preventing and fighting cyberattacks will require creativity, significant resources, and stronger partnership between the public and private sectors.

Imagine you are a corporate CEO. Your chief information security officer tells you that malicious cyber actors—possibly from China—are inside the company's networks. Whom must you notify? The answer is complicated.

- If the breach involves your customers' personally identifiable information (PII), you may be required by 50 different state laws to notify the affected individuals.[1]

- If your company is publicly traded, you face vague requirements from the Securities and Exchange Commission (SEC). Under SEC guidance issued in 2011, public companies must file a notice regarding "material" cybersecurity risks and incidents.[2] In 2018, the SEC attempted to explain

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

that materiality turns on the "nature, extent, and potential magnitude" of cybersecurity risks and incidents,[3] but it also acknowledged that "'no single fact or occurrence' is determinative as to materiality, which requires an inherently fact-specific inquiry."[4]

- On top of those requirements, if your company operates in certain industries—including finance and energy—you must notify your federal regulator of the breach.[5]

- If the breach involved personal health records, you must notify the Federal Trade Commission, the individuals whose records were affected, and the media.[6]

- Even in the absence of a statutory requirement to do so, law enforcement should also be notified. Otherwise, you may find yourself facing federal charges as Uber Technologies' former Chief Security Officer and Deputy General Counsel Joe Sullivan did. The charges against Sullivan related to his failure to report a 2016 data breach to federal investigators—without any allegation that Sullivan provided false testimony or that federal investigators even asked him about the breach.[7]

Underreporting of Cyber Breaches

These overlapping and vague requirements, combined with the natural disinclination of companies to share bad news with markets and the public, have led to the significant underreporting of cyber breaches.[8] According to one study, only 37 percent of cybersecurity breaches involving Russell 3000 companies between 2011 and 2017 were disclosed in SEC filings.[9] Companies may also be reluctant to share information related to a cyber breach with federal regulators for fear of enforcement penalties.

Chronic underreporting of cyber breaches leads to several problems. For example:

- Without information from the private sector, the federal government is poorly positioned to provide meaningful assistance, either to the company that suffered the breach or to other potential victims.[10] To be effective, experts have long recognized that this sharing must occur broadly and rapidly: Companies will be able to address common vulnerabilities only if they can patch their networks faster than attacks can exploit them.[11]

- When foreign adversaries like China or Russia are responsible for malicious cyber activity, underreporting threatens foreign policy interests. The U.S. government can deter future attacks only if it learns of past attacks in a timely fashion.

- Policymakers cannot make informed decisions about cybersecurity risks without access to accurate data on the breadth and severity of the threat.

Even when a company reports a cyber breach, information-sharing restrictions within the government frequently lead to delays and stovepipes. Take, for instance, the recent ransomware attack against Colonial Pipeline, which disrupted nearly half of the East Coast's fuel supplies. Colonial notified the Federal Bureau of Investigation (FBI), but five days after the attack, the federal entity responsible for critical infrastructure security—the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS)—had not received technical information on the hack.[12]

Law enforcement agencies like the FBI are a natural starting point for a company that suffers a breach, but the FBI's primary focus is investigating crimes, not identifying and addressing cybersecurity vulnerabilities. If other pipelines were susceptible to the same ransomware attack that Colonial suffered, it might have been days before they received the information from the federal government that would allow them to close the vulnerability. Additionally, restrictions on sharing information collected through a law enforcement investigation limit the ability of other government agencies to act on information that is reported solely to the FBI.

Congress should cut through the regulatory thicket by requiring that companies report significant cyber breaches to the federal government without fear of punishment. These reports should be minimized and anonymized to protect privacy and civil liberties and shared widely within the government in real time.

Clarifying Companies' Reporting Obligations

Federal legislation will be needed to clarify companies' reporting obligations and help the government to limit the damage from breaches. On May 12, 2021, President Joseph Biden signed an executive order recommending that the Federal Acquisition Regulation (FAR) Council consider updating the FAR to require that information technology and operational technology service providers that contract with the federal government

report cybersecurity incidents related to their work with the government.[13] While a good first step, however, the executive order fails to cover most U.S. companies, including many companies in critical sectors of the U.S. economy. The recent ransomware attack against Colonial Pipeline, for example, did not involve a federal contractor.[14] Similarly, North Korea's 2014 hack of Sony Pictures had significant consequences for U.S. cybersecurity and foreign policy, and the 2013 breach of Target's point-of-sale systems compromised the credit card information of tens of millions of Americans. Neither breach involved a federal contractor. Without additional legislative authority, President Biden's executive action will not be sufficient.

Similarly, the bipartisan recommendations of the 2020 Cyberspace Solarium Commission provide a commendable starting point for legislative proposals. The commission offered two legislative proposals, one focused on breaches of PII, the second on incident reporting for critical infrastructure.[15] A disclosure requirement for breaches of PII would help to preempt the patchwork of state data notification laws and clarify companies' reporting obligations, but like the Biden Administration's possible executive order, it does not go far enough. Standing alone, the proposal would do little to stop hacks of systems that do not handle customers' personal data. Many high-profile cyber breaches involve PII, but some of the incidents with the greatest possibility of causing catastrophic harm—like attacks against industrial control systems—do not. For instance, no PII was at issue either in the April 2020 cyberattack that, according to press reports, nearly disrupted the control systems of Israeli water treatment plants[16] or in the recent ransomware attack against Colonial Pipeline's networks.

The commission's proposed reporting requirement for critical infrastructure—a broad category that includes hotels, shopping malls, and health care[17]—is sufficiently broad in scope. Under it, the Secretary of Homeland Security, in consultation with the heads of certain sector-specific agencies (for example, the Secretary of Energy for the energy sector), must craft criteria to identify what kind of companies must report cyber incidents, what type of incidents those companies must report, and how the companies should report incidents to the federal government. In drafting these criteria, DHS should be careful to impose the smallest possible burden on the private sector by focusing on which critical infrastructure sectors and what kinds of cybersecurity incidents merit disclosure; reporting will become useless if companies report trillions of spear-phishing emails. Incident reports would be provided to CISA, which could then share the reports with other federal departments and agencies for certain purposes, including for identifying the source of the malicious activity and taking action to defend against the threat.

What Congress Should Do

Congress should go further to ensure that cyber incident reports can be used to stop future attacks before they occur. Specifically:

- Any legislation should require that information is shared within the federal government in a real-time, automated fashion. A report on a hack of power plants or water treatment facilities that arrives at CISA on a Friday evening should not wait until Monday morning to be shared with experts at the National Security Agency (NSA) and FBI who may be able to spot additional victims of the attack and advise them on how to mitigate the harm.

  CISA's Automated Indicator Sharing (AIS) system, which was authorized by the Cybersecurity Act of 2015, already enables the sharing of machine-readable cyber threat indicators,[18] and any legislation should build on that work and establish a process in which incident reports are submitted to the government confidentially but in real time. Legislation should also mirror the Cybersecurity Act's framework by requiring companies to remove extraneous personal information before they share reports with CISA, protecting companies' proprietary and privileged information, and exempting reports from federal and state open records laws.[19] Additionally, as long as information is used for an appropriate purpose—which should include identifying and preventing cybersecurity threats[20]—there should be no restrictions on which agencies of the U.S. government can receive reports from CISA.

- Legislation should require that DHS's procedures include mandatory reporting of hardware compromises and industrial control systems, not just hacks of companies' information networks. Adversaries can manipulate the supply chain for a particular product to add malicious components, or they can introduce components into a victim's network to gain access.[21] A company that discovers a malicious chip on a server's motherboard[22] or falls victim to a ransomware attack on industrial control systems for critical infrastructure[23] should be subject to the same disclosure requirements that apply to one that discovers malware on its networks.

- Legislation should not penalize companies for reporting cyber incidents. The commission's proposal prohibits private-sector reports from serving as the basis for regulation of a company, including enforcement action. Legislation should go further and eliminate existing sector-specific requirements to report breaches to regulatory agencies. For example, legislation should eliminate the Federal Energy Regulatory Commission's mandate for electric power companies to report breaches, as well as its vague requirement to report attempted breaches,[24] and obviate the need for financial services companies to notify their regulators of breaches.[25] A company that is victimized by a hack should not be required to report both to its regulators and to DHS; rather, it should file one report with DHS, which can then provide the information to all appropriate federal agencies, including regulatory agencies.

- Given recent data breach class action cases,[26] legislation should also ensure that companies are not subject to additional tort liability for reports that they make in good faith under DHS procedures. The underlying cybersecurity incident may still expose a company to liability—after all, the filing of a report should not be an excuse for negligence—but a company should not have to fear that a report to CISA would constitute evidence that the underlying cybersecurity incident resulted in material harm to the company or its customers.

- The fact of a cybersecurity incident should also not be evidence that the company failed to take reasonable precautions to defend itself against cyberattacks. Even the best-prepared company will have trouble defending itself against a sophisticated nation-state adversary. To this end, companies' reports to CISA should also be protected from disclosure in any future civil litigation. Only strong incentives to report will lead companies to disclose key information about a cybersecurity incident to the government quickly enough for it to be useful.

- Finally, like the Cybersecurity Act of 2015, any legislation should require independent reviews of the effectiveness of a disclosure mandate, as well as a sunset date to force Congress to evaluate whether the benefits of mandatory disclosure continue to outweigh the compliance cost for the private sector.[27]

Conclusion

A federal requirement to disclose cybersecurity incidents will be only a first step toward the improvement of cybersecurity defense. Cybersecurity is a complex problem that will require creative thinking, significant resources, and stronger partnership between the public and private sectors in the years ahead.[28] Congress can start down that path and help to clarify the private sector's responsibilities by enacting a single federal disclosure requirement, eliminating confusing and overlapping regulatory requirements, and providing incentives for companies to report hacks when there is still time for the government to help.

Michael Ellis is Visiting Fellow for Technology and Law in the Edwin Meese III Center for Legal and Judicial Studies, of the Institute for Constitutional Government, at The Heritage Foundation.

Endnotes

1. National Conference of State Legislatures, "Security Breach Notification Laws," April 15, 2021, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (accessed May 17, 2021).
2. U.S. Securities and Exchange Commission, Division of Corporation Finance, "CF Disclosure Guidance: Topic No. 2, Cybersecurity," October 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed May 17, 2021).
3. U.S. Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," Release Nos. 33-10459; 34-82746, applicable February 26, 2018, p. 11, https://www.sec.gov/rules/interp/2018/33-10459.pdf (accessed May 17, 2021).
4. Ibid., note 34 (quoting *Basic v. Levinson*, 485 U.S. 224, 236 (1988)).
5. See Executive Office of the President, Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, February 2018, pp. 30–31, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (accessed May 17, 2021).
6. 16 CFR Part 318, https://www.law.cornell.edu/cfr/text/16/part-318 (accessed May 17, 2021).
7. Press release, "Former Chief Security Officer for Uber Charged with Obstruction of Justice," U.S. Department of Justice, United States Attorney's Office, Northern District of California, August 20, 2020, https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-charged-obstruction-justice (accessed May 17, 2021). The charges against Sullivan for obstruction of justice and misprision of a felony relate to a hack of Uber in 2016 while the Federal Trade Commission was investigating a 2014 data breach at the company. The FTC interviewed Sullivan 10 days before the 2016 hack occurred, and Uber did not notify either the FTC or federal law enforcement of the subsequent breach. Notably, the criminal complaint does not allege that Sullivan ever represented that there had not been a subsequent data breach, and the complaint does not assert that the FTC asked Sullivan about any subsequent data breaches. See Criminal Complaint, *United States v. Sullivan*, Case No. 3-20-71168 JCS (N.D. Cal., Aug. 20, 2020), https://www.justice.gov/usao-ndca/press-release/file/1306781/download (accessed May 17, 2021).
8. See Executive Office of the President, Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, p. 30.
9. Derryck Coleman, "Nearly 65% of Affected Public Companies Did Not Report Cybersecurity Breaches to the SEC," Audit Analytics, posted February 27, 2018, https://blog.auditanalytics.com/nearly-70-of-affected-public-companies-did-not-report-cybersecurity-breaches-to-the-sec/ (accessed May 17, 2021).
10. See David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2899, April 1, 2014, http://thf_media.s3.amazonaws.com/2014/pdf/BG2899.pdf.
11. See, for example, ibid., pp. 8–11.
12. Ken Dilanian and Julia Ainsley, "Who's In Charge Here? Colonial Pipeline Hack Exposes Huge Holes in U.S. Cyber Defense, Say Experts," NBC News, May 12, 2021, https://www.nbcnews.com/news/us-news/who-s-charge-here-colonial-pipeline-hack-exposes-huge-holes-n1267057 (accessed May 22, 2021); 6 U.S.C. § 652(c), https://www.law.cornell.edu/uscode/text/6/652 (accessed May 22, 2021).
13. President Joseph R. Biden, Jr., "Executive Order on Improving the Nation's Cybersecurity, Sec. 2, Removing Barriers to Sharing Threat Information," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed May 17, 2021). See also "Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ (accessed May 17, 2021).
14. Collin Eaton and Dustin Volz, "U.S. Pipeline Cyberattack Forces Closure," *The Wall Street Journal*, updated May 8, 2021, https://www.wsj.com/articles/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline-11620479737 (accessed May 17, 2021).
15. See U.S. Cyberspace Solarium Commission, Final Report, March 2020, Recommendations 4.7.1 and 5.2.2, pp. 94 and 103–104, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (accessed May 17, 2021).
16. See Sean Lyngaas, "Israeli Official Confirms Cyberattack on Water Systems," CyberScoop, May 28, 2020, https://www.cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna/ (accessed May 17, 2021).
17. Presidential Policy Directive/PPD-21, "Critical Infrastructure Security and Resilience," The While House, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed May 17, 2021).
18. See U.S. Department of Homeland Security and U.S. Department of Justice, "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015," October 2020, https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf (accessed May 17, 2021).
19. See ibid. and 6 U.S.C. § 1503(d)(2), https://www.law.cornell.edu/uscode/text/6/1503 (accessed May 17, 2021).
20. *Cf.* 6 U.S.C. § 1504(d)(5), https://www.law.cornell.edu/uscode/text/6/1504 (accessed May 17, 2021), listing authorized purposes for use of cyber threat indicators and defensive measures shared with the federal government, including cybersecurity purposes, the purpose of identifying a cybersecurity threat, and the purposes of preventing certain serious threats and disrupting certain crimes.

21. MITRE ATT&CK, "Supply Chain Compromise," last modified January 6, 2021, https://attack.mitre.org/techniques/T1195/ (accessed May 17, 2021), and MITRE ATT&CK, "Hardware Additions," last modified April 22, 2021, https://attack.mitre.org/techniques/T1200/ (accessed May 17, 2021).
22 . See, for example, Jordan Robertson and Michael Riley, "The Long Hack: How China Exploited a U.S. Tech Supplier," Bloomberg, February 12, 2021, https://www.bloomberg.com/features/2021-supermicro/ (accessed May 17, 2021), describing the discovery of a malicious component on motherboards manufactured in China by the U.S. company Supermicro.
23. See, for example, Cynthia Brumfield, "Colonial Pipeline Shutdown Highlights Need for Better OT Cybersecurity Practices," *CSO*, May 10, 2021, https://www.csoonline.com/article/3618016/colonial-pipeline-shutdown-highlights-need-for-better-ot-cybersecurity-practices.html (accessed May 17, 2021).
24. U.S. Department of Energy, Federal Energy Regulatory Commission, "Cyber Security Incident Reporting Reliability Standards," Final Rule, July 19, 2018, *Federal Register*, Vol. 83, No. 147 (July 31, 2018), pp. 36727–36741, https://www.govinfo.gov/content/pkg/FR-2018-07-31/pdf/2018-16242.pdf (accessed May 24, 2021).
25. U.S. Department of the Treasury, Office of the Comptroller of the Currency; Federal Reserve System; and Federal Deposit Insurance Corporation, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," Proposed Rule, *Federal Register*, Vol. 86, No. 7 (January 12, 2021), pp. 2299–2311, https://www.occ.gov/news-issuances/federal-register/2021/86fr2299.pdf (accessed May 24, 2021).
26. See, for example, *In re Yahoo! Inc. Shareholder Litigation*, Case No. 17-CV-307054 (Cal. Sup. Ct., Santa Clara Co., Jan. 4, 2019), and *In re Equifax Inc. Securities Litigation*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019).
27. See 6 U.S.C. § 1506, https://www.law.cornell.edu/uscode/text/6/1506 (accessed May 22, 2021); 6 U.S.C. § 1510, https://www.law.cornell.edu/uscode/text/6/1510 (accessed May 22, 2021).
28. See, for example, Dustin Carmack and Chad F. Wolf, "How to Strengthen America's Cyberdefenses," Heritage Foundation *Commentary*, March 18, 2021, https://www.heritage.org/cybersecurity/commentary/how-strengthen-americas-cyberdefenses.