CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

ASPEN
DIGITAL
aspen institute

MARCH 2022

Cybersecurity Is a Team Sport: Bolstering How U.S. Federal and State Officials Share Incident Information

R. Taj Moore

Cybersecurity Is a Team Sport: Bolstering How U.S. Federal and State Officials Share Incident Information

R. Taj Moore

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction

To understand and respond effectively to the threats posed by malicious hackers, the U.S. government needs more data and quickly. While the situation is improving, according to Deputy Attorney General Lisa Monaco, "[M]ost breaches are not reported to law enforcement."[1] As a result, the federal government is essentially flying blind when combating cyber threats. A new federal reporting requirement has been included in the $1.5 trillion omnibus spending bill that the House of Representatives passed on March 9, 2022, though the bill has not yet passed in the Senate. [2] In the meantime, and even after this bill passes, more comprehensive information-sharing channels between the federal government and the fifty states could help.

As Monaco recently wrote in an op-ed calling for congressional action, without prompt reporting of cyber attacks, the federal government is unable to see "the full picture of the threat facing our country," and its power to counter "all cybercriminal activity" diminishes.[3] The deputy attorney general isn't alone in the view that a breach-reporting requirement could help enable government action. During a November 2021 U.S. House Committee on Homeland Security hearing, Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly said that, while CISA was grateful for the many authorities provided to it, "[W]e appreciate what's in potential upcoming legislation to include cyber-incident reporting."[4] (That's polite Washington speak for "we really need an incident reporting law.") Members of Congress have taken steps to develop such a requirement, but recent attempts have hit roadblocks.[5] In the meantime, to help close this information gap, federal officials are searching for new tools. One important yet underused tool is the federal government's partnerships with state governments.

Recent news reports suggest that the Department of Justice will begin to use the False Claims Act to compel federal contractors to disclose "significant" security breaches.[6] Using this law is a start, but this approach has its limits. First, the False Claims Act would offer only a partial picture of the threat landscape because, as used in this context, it would capture information only from contractors and other parties engaged in or seeking transactions or contracts with the federal government.[7] Second, it might not fulfill the need for prompt reporting given inefficiencies in the existing government contracts process.

Until Congress answers the deputy attorney general's call to enact "legislation to create a national standard for reporting cyber incidents that pose significant risk, including ransomware and incidents that affect critical infrastructure and their supply chains," there are additional fixes that the government could rely on.[8] Specifically, the federal government could turn to its state-level partners to help fill some information gaps. Even if Congress ultimately enacts a breach-reporting requirement for operators of critical infrastructure and a broader set of ransomware victims, states can help key federal agencies learn about a variety of security incidents and potentially filter out less significant cases.[9] This way, the federal government can focus on the most critical security threats while state governments can address others. This kind of partnership would likely require appropriate funding but, if done right, it would be a worthy investment.

Why Incident Reporting Matters

Without good data, federal government officials are less capable of effectively responding to cyber threats and they are more likely to repeat mistakes. Public reporting or companies' own general disclosures of cybersecurity incidents long after they occur are insufficient. Newspaper reports, for example, might share some general information about what happened during an incident, but the federal government might have technical questions only the victim of the attack can answer. Or, even if those details are made public (in an accurate way), it might be too hard for federal officials to piece together the full story based on such reporting. Additionally, if the federal government learns about an attack after the fact, it will have lost the time it needs to share common technical vulnerabilities widely and to develop effective countermeasures. While several information-sharing organizations seek to disseminate data on known vulnerabilities and cyber attacks, they are generally focused on their own specific sectors (such as financial services, information technology, healthcare, space, and others) and depend on voluntary participation.[10] The same is true of the Joint Cyber Defense Collaborative. While it provides a helpful forum for private-sector entities to share information with the federal government, it remains a coalition of the willing and thus

provides an incomplete picture of the threat landscape.

By contrast, the federal government—if it has the full picture—is unique in its ability to transcend sectoral divides, identify threat patterns that exist within and beyond specific industries, bring charges against cybercriminals where applicable (yes, sometimes it happens),[11] and develop strategic responses to broader national security and foreign policy challenges.[12]

In short, adequate incident reporting is not an accessory to combating cybersecurity threats—it is indispensable to that goal. Although insufficient on its own, appropriate information sharing can help enable the effective use and measurement of all other policies designed to protect against cyber attacks, including defensive measures, offensive operations, and geopolitical agreements. Forging a solution, and measuring its efficacy, requires the full set of facts, which the U.S. government currently does not have.

Ongoing Russian aggression against Ukraine provides an important illustration of how valuable timely information sharing can be. White House officials suspected early on that the Russian offensive would involve cyber attacks designed to destabilize Ukraine.[13] Even though the United States might not be a direct and immediate target of a cyber attack at this stage of the conflict, it is possible that Russia is planning for the current crisis to escalate even further. In that scenario, Russia would likely want to be in a position to hit the United States where it hurts—specifically by attacking operators of critical infrastructure. As of now, private-sector entities manage "a vast majority of the [United States'] critical infrastructure."[14]

Because many of the country's richest targets are privately held, the U.S. federal government might not have the earliest insights into cyberactivity on those networks, but the private sector could make relevant observations. Right now, there is no general federal requirement that these high-value targets report information about known or potential incidents, which means that the federal government simply has to hope that its private-sector partners feel compelled to report out of a sense of good citizenship. If these companies were required to report "significant" activity to the federal government, it is possible federal officials would have better insights into Russian operational-preparation-of-the-environment (OPE) activities, which would help the U.S. government better prepare for conflict before an actual attack.[15]

Incident reporting should not be overly burdensome on companies, and it should not require firms to report more information than is strictly necessary, but such reporting does need to happen. With time, the particulars of reporting requirements can be reformed so they are workable for industry actors and responsive to evolving threats.

Enhancing Cyber Information Sharing Between the Federal Government and States

There are multiple ways that the federal government could consider expanding information sharing with state governments on cyber incidents, but the most straightforward approach would likely be to establish formal channels for state officials to share information on cyber incidents that they already collect. Ideally, key states could revise their breach-notification laws to cover "significant" events involving federally designated critical infrastructure and other incidents of interest to federal officials, such as ransomware attacks.

Rely on Existing State Laws on Breach Notices

Unlike the federal government, the vast majority of U.S. states already have breach-notification laws in place. Many of these laws require that breached companies provide notice to state governments in addition to impacted individuals.[16] A key downside is that the notice triggers for many of these statutes are based on variables that are typically more important to consumers than to national security officials, such as the kinds of personal information impacted as well as the location and number of impacted individuals. Notably, these laws generally do not cover attacks to critical infrastructure that do not affect personal data.

In New Jersey, for instance, any business or public entity that "compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."[17] Before notice is provided to affected consumers, however, the impacted entity must report the breach to the New Jersey Department of Law and Public Safety, which retains the power to disseminate or refer the information "to other appropriate law enforcement entities."[18] That term is undefined in the statute but could arguably include federal law enforcement officials.

Other laws differ. In the West Virginian statute, for example, there is no express language about sharing data with appropriate law enforcement officials, and unlike in the New Jersey law, notice hinges on a reasonable prospect of "identity theft or other fraud" materializing.[19] West Virginia's statute does, however, touch on the involvement of law enforcement, as it states that a notice to individuals can be delayed if an agency determines that "notice will impede a criminal or civil investigation or homeland or national security."[20] Still, the onus is on enforcement officials to learn independently about what is going on and make a determination.

In short, state laws differ in meaningful ways with respect to whom notice should be provided to, how it should be given, and what triggers notice in the first place—and these laws generally do not cover security incidents that affect critical infrastructure or their supply chains. As a result, relying solely on reporting in compliance with existing state statutes provides only a partial picture of the security threats facing the nation.

Nonetheless, collecting and assessing state data would be a helpful start as national security officials seek to assemble a broader mosaic of cybersecurity activities. Incidentally, such a move would also capture some threat events of interest to the federal government. Accessing information already collected by the fifty states—or at least a subset of states with jurisdiction over critical infrastructure and other vital industries—is one meaningful option for the executive branch as it waits to see if Congress will enact a federal requirement for breach notifications.

Expand Existing State Laws on Breach Notices

Relying on existing state laws on breach notifications should be the floor, not the ceiling. Ambitious state governments could proactively amend their existing statutes to include "significant" events involving federally designated critical infrastructure, a move that would better serve everyone's security priorities. If, for instance, New Jersey wanted to make sure its breach-notification law covers such incidents, it could amend the law to include events that affect federally designated "critical infrastructure." It could then pass along to the federal government the information federal officials need to begin sharing vulnerabilities and attacker information with critical infrastructure operators nationally and to craft effective responses to cyber threats. Importantly, many state legislatures do not face the kind of gridlock that Congress does, which may make state legislators more likely to enact the requisite requirements in a timely manner.[21]

Moreover, not all U.S. states would need to amend their breach-notification statutes for the federal government to get the insights it needs. State governments with jurisdiction over key companies and industries—such as California, Delaware, New Jersey, and New York—could be candidates of such partnerships.

Joint Cybersecurity Task Forces

Officials already have several models for federal-state partnerships to learn from. The National Cyber Investigative Joint Task Force, for instance, was established in part to leverage "the collective authorities and capabilities of its members" and to coordinate "with international and private sector partners to bring all available resources to bear against domestic

cyber threats and their perpetrators."[22] While the task force might not be the appropriate forum for a federal-state partnership given its emphasis on federal-level coordination, it is one example of how information sharing that is designed to leverage the various authorities of different entities can be used to coordinate and respond to cybersecurity threats.

Joint terrorism task forces would be another model to consider. These consist of "locally based, multi-agency teams of investigators, analysts, linguists, SWAT experts, and other specialists who investigate terrorism and terrorism-related crimes."[23] A collection of select joint cybersecurity task forces could exist across the nation or solely in critical jurisdictions. They could be co-led by local Federal Bureau of Investigation (FBI) field offices and a CISA representative, and they could include state and local cyber officials; state-level law enforcement officers; and relevant federal representatives from the Department of Justice, the FBI, and the Secret Service. As a young organization with less reputational baggage than some of its peers, CISA might be best suited to build trust among participants and act as an honest broker.

Together, these experts could collect evidence, disseminate it appropriately, take official action consistent with their authorities, respond to threats at a moment's notice, and feed information to the National Cyber Investigative Joint Task Force and other entities as appropriate.[24] This could also help reduce the chances that duplicative investigations occur at various levels involving state and federal government officials. Joint cybersecurity task forces would not be responsible for affirmative incident response that victims usually control, but they would be tasked with leveraging information to take proactive steps to protect as many entities as possible and try to hold malicious actors accountable without delay.

Additionally, and even if Congress does eventually pass a federal breach-notification bill, a prospect that seems increasingly likely, joint cybersecurity task forces could remain useful to the extent that they can reduce the federal government's reporting burden by allowing a joint team of state and federal officials to filter out incident reports that are less important to national security.[25]

Align Activities With States' Interests

This approach would also serve the interests of state governments. First, it would empower state officials, including state attorneys general and prosecutors, to understand the full range of criminal activity occurring within their borders that might be worthy of prosecution. Second, it would allow them to take steps to protect major employers who could be crippled by a severe malicious attack, which could have ripple effects on a state's economy (and a governor's agenda and election prospects).

This might not be enough to convince state governments to sign up. They might worry that any partnership with the federal government, even informal, would be burdensome. Even if they are willing, they might not have the financial or personnel resources necessary to

allocate and share a broader swath of data. In all likelihood, an appropriation of some kind would be necessary to make this kind of partnership productive. But in light of the critical threat facing the nation, the investment could be a worthy one.

Conclusion

Improved information sharing via robust federal-state partnerships is not the antidote to the country's cybersecurity problems. Even with a better understanding of the problem, government officials will still face questions of what an effective response looks like and how to achieve it. But the United States needs to be able to measure which policies work and which ones do not. Currently, the federal government is not in a position to do so.

Developing an appropriate strategic remedy starts with an accurate diagnosis of the full threat. Bolstering the federal-state information-sharing apparatus would help the executive branch as Congress works on a national reporting requirement, and it could be part of an effective, whole-of-society approach to combating cyber attacks against the United States.

About the Author

R. Taj Moore is director of the Aspen Cybersecurity Group, an initiative of Aspen Digital. He recently worked as an associate at Morrison and Foerster LLP, where he advised companies on how to prepare for and respond to cyber attacks executed by cyber criminals and other adversaries. He previously served as assistant counsel to Governor Philip D. Murphy of New Jersey, as a Lawfare contributor, and as a Scoville Fellow at the Stimson Center. He is co-author of "Balancing Privacy and Public Safety in the Post-Snowden Era," published in the *Cambridge Handbook of Surveillance Law* (Cambridge University Press, 2017).

Notes

1 Lisa Monaco, "America Needs Congress's Help to Solve the Ransomware Threat," CNBC, October 6, 2021, https://www.cnbc.com/2021/10/06/deputy-ag-congress-must-create-standard-to-encourage-companies-to-report-cyberattacks.html.

2 Melissa Quinn, "House Passes $1.5 Trillion Omnibus Spending Package, With $13.6 Billion in Ukraine Aid," CBS *News*, March 9, 2022, https://www.cbsnews.com/news/house-vote-spending-bill-ukraine-aid.

3 Ibid.

4 "House Homeland Security Committee Hearing on Cybersecurity Efforts," 117th Cong. (2021), (testimony of CISA director Jane Easterly, November 3, 2021,), https://www.c-span.org/video/?515816-1/house-homeland-security-committee-hearing-cybersecurity-efforts. See the 28:25 timestamp.

5 Tim Starks, "Cyber Incident Reporting Mandates Suffer Another Congressional Setback," Cyberscoop, December 7, 2021, https://www.cyberscoop.com/cyber-incident-reporting-ransomware-payments-congress-ndaa; and Tim Starks, "Incident Reporting, Ransomware Payment Legislation Faces Trouble in Senate," Cyberscoop, November 24, 2021, https://www.cyberscoop.com/incident-reporting-ransomware-payment-legislation-senate-scott-amendment.

6 Eric Tucker, "US Poised to Sue Contractors Who Don't Report Cyber Breaches," AP News, October 7, 2021, https://apnews.com/article/technology-business-lisa-monaco-statutes-government-grants-1772e6cc6c3f686f26e2ab1e4ebcb39b. The False Claims Act was enacted to address contractor fraud by imposing a penalty on any person who knowingly submitted false claims to the government. Department of Justice, "The False Claims Act," Department of Justice, February 2, 2022, https://www.justice.gov/civil/false-claims-act.

7 31 U.S. Code § 3729, Cornell Law School, https://www.law.cornell.edu/uscode/text/31/3729.

8 Monaco, "America Needs Congress's Help to Solve the Ransomware Threat."

9 CISA, "List of Critical Infrastructure Sectors," CISA, https://www.cisa.gov/critical-infrastructure-sectors.

10 Financial Services Information Sharing and Analysis Center (FSISAC), "Who We Are," FSISAC, https://www.fsisac.com; Information Technology Information Sharing and Analysis Center (IT-ISAC), "FAQ," IT-ISAC, https://www.it-isac.org/faq; Health Information Sharing and Analysis Center (H-ISAC), "H-ISAC Frequently Asked Questions," H-ISAC, https://h-isac.org/h-isac-faq; and Space Information Sharing and Analysis Center (S-ISAC), "About Space ISAC," S-ISAC, https://s-isac.org/about-us.

11 U.S. Department of Justice, "Russian National Extradited to United States to Face Charges for Alleged Role in Cybercriminal Organization," U.S. Department of Justice (press release), October 28, 2021, https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal.

12 Sometimes, what appears to be a run-of-the-mill hack unworthy of government attention could have enormous implications on other national security investigations. See John P. Carlin and Garrett M. Graff, *Dawn of the Code War* (New York: Public Affairs, 2018). In this book, the authors highlight a 2015 case where an individual based in Malaysia hacked an online retailer in Illinois, taking the credit card and email information of over 100,000 individuals. The hacker then shared that information with the self-proclaimed Islamic State, which used it as a basis for a kill list.

13 David E. Sanger, "U.S. Sends Top Security Official to Help NATO Brace for Russian Cyberattacks," *New York Times*, February 1, 2022, https://www.nytimes.com/2022/02/01/us/politics/russia-ukraine-cybersecurity-nato.html.

14 CISA, "Critical Infrastructure Sector Partnerships," CISA, https://www.cisa.gov/critical-infrastructure-sector-partnerships.

15 Of course, for this approach to work, the definition of "significant" would have to be designed to include OPE activity.

16 "Security Breach Notification Chart, Perkins Coie (last updated September 2021), https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf"

17 NJ Rev Stat § 56:8-163(a)-(b), Casetext, https://casetext.com/statute/new-jersey-statutes/title-56-trade-names-trade-marks-and-unfair-trade-practices/chapter-568/section-568-163-disclosure-of-breach-of-security-to-customers. According to the law, a "breach of security" is defined as an "unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable."

18 Ibid. See NJ Rev Stat § 56:8-163(c). For states without explicit language about transferring data to "other appropriate law enforcement entities," there does not appear to be a clear restriction on the ability of state governments to share breach data with federal law enforcement officials. However, out of an abundance of caution, such states could amend their statutes to authorize such sharing.

19 See West Virginia Code § 46A-2A-102(a), West Virginia Legislature, https://code.wvlegislature.gov/46A-2A-102.The law states, "An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this State whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person ***and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this State.***" (emphasis added)

20 Ibid. See West Virginia Code § 46A-2A-102(e).

21 Glen Justice, "States Six Times More Productive Than Congress," Congressional Quarterly, January 27, 2015, (last visited March 3, 2021), https://info.cq.com/resources/states-six-times-more-productive-than-congress. (This piece suggests that, with respect to the number of bills passed, state legislatures are more productive than Congress.) Also see Quorum, "State Legislatures vs. Congress: Which Is More Productive?" Quorum, https://www.quorum.us/data-driven-insights/state-legislatures-versus-congress-which-is-more-productive.

22 FBI, "National Cyber Investigative Joint Task Force," FBI, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

23 Jerome P. Bjelopera, "The Federal Bureau of Investigation and Terrorism Investigations," Congressional Research Service, April 24, 2013, https://sgp.fas.org/crs/terror/R41780.pdf.

24 FBI, "Joint Terrorism Task Forces," FBI, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces.

25 Tim Starks, "Proposal for Industries to Report Big Cyberattacks, Ransomware Payments Wins Senate Approval," Cyberscoop, March 2, 2022, https://www.cyberscoop.com/cyber-incident-reporting-passes-senate.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decision-makers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

TIA's work informs and is informed by direct dialogues among thought-leaders, senior officials, and executives in key countries. We share the data, insights, and policy recommendations that result in reports, commentaries, and web tools. Carnegie's regional centers and networks in the United States, China, Europe, India, and Russia provide a widely respected international platform for promoting our policy proposals.

Aspen Institute

The Aspen Institute is a global nonprofit organization committed to realizing a free, just, and equitable society. Founded in 1949, the Institute drives change through dialogue, leadership, and action to help solve the most important challenges facing the United States and the world. Headquartered in Washington, DC, the Institute has a campus in Aspen, Colorado, and an international network of partners.

Aspen Digital Program

Aspen Digital empowers policy-makers, civic organizations, companies, and the public to be responsible stewards of technology and media in the service of an informed, just, and equitable world. This Aspen Institute program shines a light on urgent global issues across cybersecurity, the information ecosystem, emerging technology, the industry talent pipeline, tech and communications policy, and innovation. It then turns ideas to action and develops human solutions to these digital challenges.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org

ASPEN DIGITAL
aspen institute

AspenInstitute.org