THE CRITICALITY OF COORDINATED DISCLOSURE IN MODERN CYBERSECURITY

Prepared by the Energy and Commerce Committee, Majority Staff

October 23, 2018 White Paper Series energycommerce.house.gov

Introduction

Over the past several years, the Committee on Energy and Commerce has conducted oversight of cybersecurity strategies and incidents both at federal agencies and in the private sector. As part of that work, the Committee has examined the cybersecurity capabilities of the automotive industry, sought and received comment regarding the risks of legacy technologies in the healthcare sector, studied the prevalence and associated policy implications of the use of open-source software in modern software development, and much more.[1]

One of the first patterns that emerged as the Committee carried out this work is that, often, organizations do not discover incidents on their own—they are told by outside parties. These third-parties may be law enforcement officials, business partners, financial firms, or—as is increasingly the case—independent security researchers. This process, known as coordinated disclosure, has existed as a well-known but controversial cybersecurity strategy for nearly two decades. Some organizations not only accept but welcome third-party investigation of their cybersecurity postures, while others reject such assistance and, in certain cases, pursue civil or criminal charges against the parties presenting the information.

The Committee's work has shown that the complexity of modern information systems and networks makes coordinated disclosure an essential, rather than optional, part of an organization's overall cybersecurity strategy. This fact is demonstrated by the increasing number and frequency of significant coordinated disclosures, highlighted most recently by the Spectre and Meltdown disclosures that impacted nearly every modern technology that relies on computer chips. As the Committee's investigation into that disclosure showed, not only is coordinated disclosure critically important, its criticality necessitates that society move past a debate of whether coordinated disclosure is "good" or "bad" and instead focus on how disclosure processes may be meaningfully improved.[2]

This White Paper begins with a discussion of the complexity of the Internet and other modern information systems and networks and explores how and why that complexity requires organizations to embrace coordinated disclosure. Next, it provides an overview of how coordinated disclosures typically proceed and explores what types of organizations now recommend or have adopted such programs. The White Paper then examines challenges and opportunities that remain regarding the adoption of coordinated disclosure, including the uncertain legal environment in which programs and participants must operate and the negative public perceptions with which they must contend. Finally, it details recommendations regarding coordinated disclosure based on the Committee's body of work on this topic specifically and cybersecurity issues generally.

[1] Letters from the Hon. Fred Upton, Hon. Frank Pallone, Jr., Hon. Joe Barton, Hon. Diana DeGette, Hon. Marsha Blackburn, Hon. Anna G. Eshoo, Hon. Tim Murphy, Hon. Jan Schakowsky, Hon. Greg Walden, and Hon. Michael C. Burgess, H. Comm. on Energy and Commerce, to the Nat. Highway Traffic Safety Admin., General Motors, Ford, FCA North America, Toyota, Honda, Nissan, Hyundai, Mazda, Mitsubishi, Kia, Subaru, Mercedes Benz, Vovlo, Volkswagen, Audi, Porshe, and Tesla (May 25, 2015); *Supported Lifetimes Request for Information*, H. Comm. on Energy and Commerce (Apr. 20, 2018); Letter from the Hon. Greg Walden and Hon. Gregg Harper, H. Comm on Energy and Commerce, to Jim Zemlin, the Linux Foundation (Apr. 2, 2018).

[2] Letter from the Hon. Greg Walden, Hon. Marsha Blackburn, Hon. Robert E. Latta, and Hon. Gregg Harper, H. Comm on Energy and Commerce, to Apple, Amazon, AMD, ARM, Google, Intel, and Microsoft (Jan. 24, 2018).

Society's integration with and resultant dependency on the Internet and connected technologies will only continue to grow, and with that growth comes a corresponding increase in the complexity of information systems and networks. Consequently, as the Committee's investigation into cybersecurity strategies and incidents have shown, coordinated disclosure may no longer be considered just one of many possible facets of an organization's cybersecurity program, but an indispensable cornerstone.

Part I – The Internet, Complexity, and "Unknown Unknowns"

One of the first patterns that emerged as the Committee began to analyze cybersecurity incidents is that, often, organizations do not discover incidents on their own—they are told by outside parties. Whether organizations learn about incidents through law enforcement officials made aware of compromises through ongoing monitoring of criminal communications, financial partners made aware due to fraud controls, or security researchers made aware during research, third-party disclosure is an element that has appeared again and again in incidents, in companies of all sizes and across all industries.

Statistical data bears this out. Both the 2016 and 2017 Verizon Data Breach Investigations Reports document this trend:[3]

Figure 1 - Breach Discovery Methods Over Time

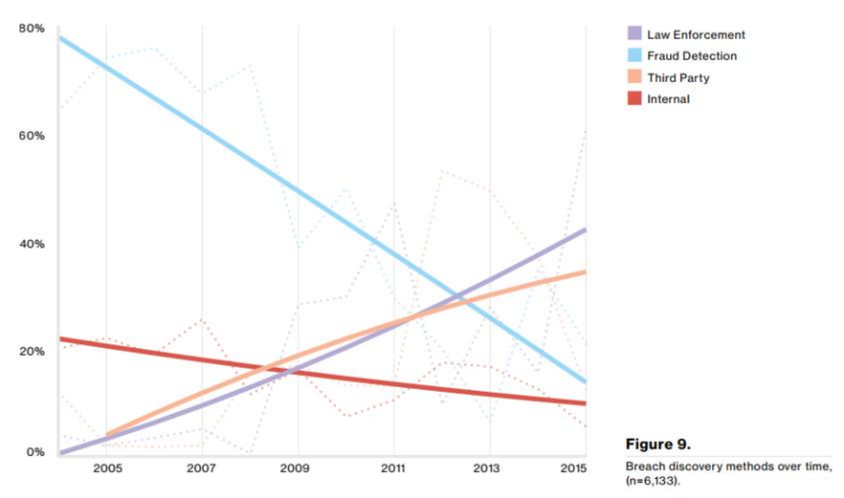

Figure 1 from *2016 Verizon DBIR*, note 1, at 15.

[3] *2016 Data Breach Investigations Report*, Verizon (last visited Jan. 18, 2018), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (hereafter *2016 Verizon DBIR*); *2017 Data Breach Investigations Report*, Verizon (Apr. 20, 2017) (hereinafter *2017 Verizon DBIR*).

Figure 2 - Breach Discovery Methods Over Time

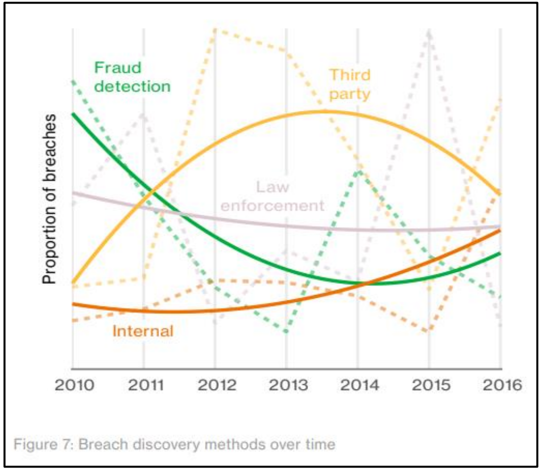

Figure 2 from *2017 Verizon DBIR*, note 1, at 10.

The barest glance "under the hood" at the modern information technology (IT) ecosystem shows why. Take what appears to be a two-step process of opening a link to a website; a user clicks on the link, and then the website opens. In fact, as Figure 3 illustrates, this process requires dozens of steps and individual technology components.[4]

Figure 3 - Flowchart of a Website Request

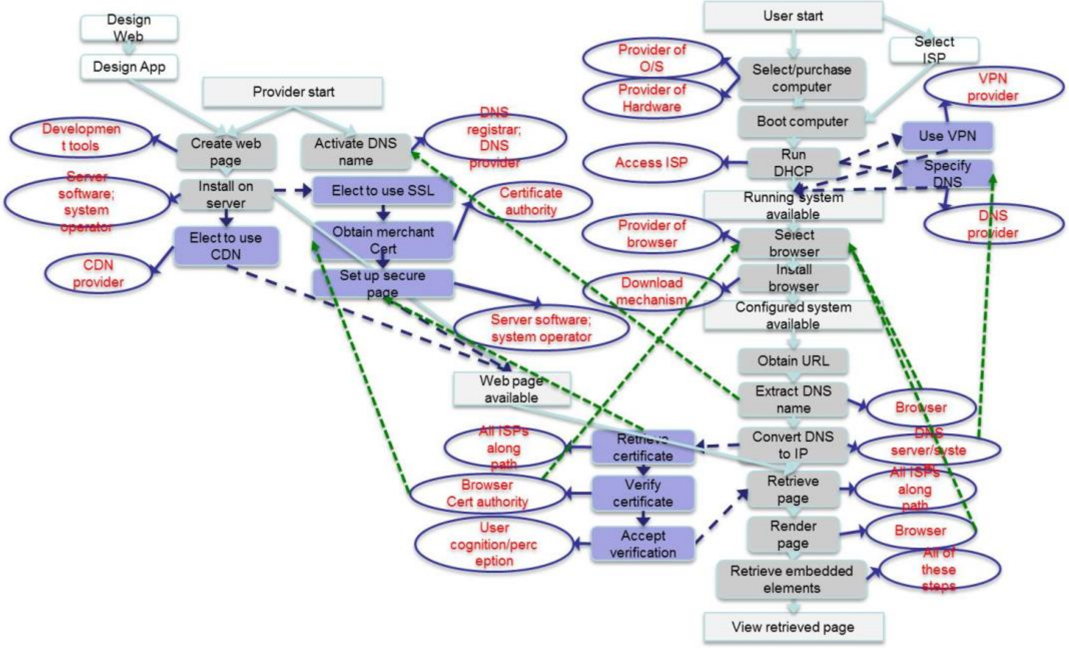

Figure 3 from *Primer*, note 2, at 39.

[4] COMMITTEE ON DEVELOPING A CYBERSECURITY PRIMER: LEVERAGING TWO DECADES OF NATIONAL ACADEMIES WORK, NATIONAL ACADEMY OF SCIENCES, AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY: SOME BASIC CONCEPTS AND ISSUES 21 (David Clark et al. eds., 2014), *available at* http://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic (hereinafter *Primer*).

Further, this flowchart represents *only* the steps necessary to open a web page. Imagine the potentially hundreds of individual steps that must successfully be completed before an online bank transaction occurs, an electronic health record opens, or instructions are delivered to a piece of industrial control systems (ICS) equipment. If any of these steps fail, the requested action itself likely fails in its entirety. Misconfigurations, coding errors, security vulnerabilities, and unforeseen issues with each individual component may all cause such failures.

Modern information systems now contain hundreds, if not thousands, of these individual software and hardware components. Further, these components—while perhaps identical to one another in isolation—are then combined in entirely unique ways from organization to organization. Consequently, no two IT configurations are the same. This creates severe challenges for organizations trying to manage their IT needs and risks, as standardized compliance frameworks or strategies may only ever be partially applicable. Organizations are thus often required to develop unique policies and procedures that apply specifically to their own internal IT systems, and to do so nearly from scratch.

The complexity continues from there. The evolution of modern IT and the intrinsic interconnection of systems means that thinking of an organization as having its own "network" or isolated IT system is woefully outdated. The IT presences of organizations today are so heavily integrated with those of their partners, their suppliers, their customers, and sometimes even their regulators that they are, in essence, all part of one network. As a result, no one organization can feasibly be expected to understand the true shape and scope of its own IT presence and exposure, since doing so would inevitably involve simultaneously understanding the entirety of any network connected to it.

This is an uncomfortable truth, and one that runs counter to many cybersecurity best practices, each of which almost inevitably requires a full accounting of an organization's assets and a comprehensive understanding of the risks it faces. While this is an necessary component of any mature cybersecurity program and one that each organization should strive to meet, the Committee's cybersecurity work has shown that it is ultimately a Sisyphean task. Due to the complexity of modern information systems—which is growing exponentially as society becomes more entwined with technology and the Internet—there are too many "unknown unknowns." As such, organizations require a mechanism through which they may eliminate as many of those unknown unknowns as possible.

Part II – The Adoption of Coordinated Vulnerability Disclosure Programs

Looking at some of the largest cybersecurity incidents in recent history, many organizations became aware of cybersecurity incidents either upon receiving a victim notification from a law enforcement agency or because of anti-fraud measures. These types of disclosures are generally both well-understood and noncontroversial and, while an important factor in cybersecurity awareness, their limited scope tends to restrict their utility to either large criminal campaigns or breaches of financial or personally-identifiable information. As a result, neither encompasses a separate, growing, and more complicated type of disclosure: those made by independent third-parties.

Third-party disclosures are typically broken into two categories; public vulnerability disclosures and coordinated vulnerability disclosures (CVD). In the first, third-parties publish cybersecurity incident data in a public forum, usually without providing advanced notice to the affected organization. While there are occasionally sound reasons for third-parties to perform public disclosures, the potential consequences are obvious. Releasing details on cybersecurity incidents without giving the affected organization time to prepare may impact that organization's ability to provide user support or, in the case of cybersecurity vulnerability information, may give malicious actors an opportunity to exploit the information before the organization can provide technological mitigations or fixes.

CVD, on the other hand, involves collaboration between the third-party disclosing vulnerability information and the affected organization.[5] These third-parties typically provide the vulnerability information privately at first to give the affected organizations time to confirm the issue, as well as to develop and deploy fixes, thus minimizing the potential impact of the vulnerabilities.[6] Once such a fix is ready and distributed, either the third-party, the organization, or both, often publicly acknowledge the vulnerability, the contributions of the third-party, and the availability of the fix.[7]

CVD has already proven its worth several times over. In the last few years alone, several high-profile disclosures have led to the identification, mitigation, or elimination of cybersecurity vulnerabilities in traditional IT, medical devices, ICS equipment, Internet-of-Things products, and more.[8] In January 2018, for example, one of the largest known CVDs was made public when several technology companies announced that they had been working together for nearly six

CVD vs. "Bug Bounties"

A common point of confusion around CVD is CVD's relationship to "bug bounties." The two are similar, but with several critical distinctions. First and foremost, an organization through a bug bounty typically offers a reward—money, "swag," etc. —for third-parties who report vulnerabilities. Second, a bug bounty is usually seen as an explicit invitation or solicitation for vulnerability information. CVD programs, on the other hand, do not necessarily offer rewards, nor do they necessarily "invite" research or investigation. Instead, they outline what types of research or investigation an organization will accept, how to contact an organization should relevant vulnerability information be discovered, and the process that an organization will follow to respond to and remediate vulnerabilities. A bug bounty may be considered a specific type of CVD program, but an organization does not need to offer rewards or explicitly invite research or investigation to have an effective CVD program.

[5] Allen D. Householder et al., *The CERT® Guide to Coordinated Vulnerability Disclosure*, SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY 9 (2017), https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

[6] *Id.*

[7] *Id.*

[8] Tod Beardsley, *R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump*, RAPID7 (Oct. 4, 2016), https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/; *ICS-CERT Advisories*, ICS-CERT (last visited Feb. 6, 2018), https://ics-cert.us-cert.gov/advisories; Danny Palmer, *Vulnerabilities in these IoT cameras could give attackers full control, warn researchers*, ZDNET (June 18,

months to mitigate critical vulnerabilities identified in nearly all modern computer chips through a multi-party CVD.[9]

Each of these cases of CVD involved different vulnerabilities, reported to different companies, by different third-parties. Nevertheless, the result of each was the improved security and safety of the affected products, which in turn improves the security and safety of technology overall and of the individuals and organizations that rely upon them.

In recognition of this fact, many organizations recommend or have adopted coordinated disclosure programs.[10] For example, in the public sector:

- The Department of Defense (DOD) established a CVD program for the DOD enterprise in spring of 2016 and is now working with other federal agencies to develop similar programs.[11]

- The Department of Justice (DOJ) issued a framework in July 2017 for use by organizations to help them design CVD programs whose policies "substantially reduce[] the likelihood that [CVD activities] will result in a civil or criminal violation of law[.]"[12]

- The Food and Drug Administration (FDA), in their 2016 "Postmarket Management of Cybersecurity in Medical Devices," specifically includes adoption of CVD programs as a "critical component" of a medical device manufacturer's overall cybersecurity risk management program.[13]

- The National Highway Traffic Safety Administration (NHTSA) stated in its October 2016 "Cybersecurity Best Practices for Modern Vehicles" that, "NHTSA supports additional mechanisms for information sharing, such as a vulnerability reporting/disclosure program."[14]

2018), https://www.zdnet.com/article/vulnerabilities-in-these-iot-cameras-could-give-attackers-full-control-warn-researchers/.

[9] Peter Bright, *Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it,* ARS TECHNICA (Jan. 5, 2018), https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/.

[10] *US Government ❤ Coordinated Disclosure*, I AM THE CAVALRY (last visited Feb. 6, 2018), https://www.iamthecavalry.org/usgdisclosure.

[11] *Hack the Pentagon*, DEPT. OF DEFENSE (last visited July 16, 2018), https://www.hackerone.com/resources/hack-the-pentagon.

[12] *A Framework for a Vulnerability Disclosure Program for Online Systems*, DEPT. OF JUSTICE (last visited July 16, 2018), https://www.justice.gov/criminal-ccips/page/file/983996/download.

[13] *Postmarket Management of Cybersecurity in Medical Devices*, FOOD & DRUG ADMIN. (last visited July 16, 2018), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

[14] *Cybersecurity Best Practices for Modern Vehicles*, NAT. HIGHWAY & TRAFFIC SAFETY ADMIN. (last visited July 16, 2018), https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity#resources.

- The National Institute of Standards and Technology (NIST) added a section to its December 2017 revision of the "Cybersecurity Framework" regarding CVD.[15]

- The National Telecommunications and Information Administration (NTIA) undertook a multi-month process from July 2015 to December 2016 to explore CVD challenges and opportunities, culminating in several CVD documents and guidelines.[16]

- The Patent and Trademark Office (PTO) issued exemptions for liability for the Digital Millennium Copyright Act (DMCA) for certain types of vulnerability research in 2016. The PTO is currently considering whether to expand the exemption to additional types of research.[17]

Similarly, the following private sector organizations, among numerous others, have established CVD programs:

- Auto manufacturers Fiat Chrysler Automobiles, General Motors, TESLA, and Toyota;[18]

- Critical infrastructure manufacturers GE, Panasonic Avionics, and Siemens;[19]

- IT sector companies Amazon, Google, Intel, and Microsoft, among numerous others;[20]

- Medical technology manufacturers Abbott, BD, Beckman Coulter, Boston Scientific, Draeger, GE, Johnson & Johnson, Medtronic, Orion Health, Philips, Saint Jude Medical, Siemens, Stryker, and Tidepool.[21]

[15] *Framework for Improving Critical Infrastructure Cybersecurity*, NAT. INST. OF SCIENCE AND TECH. (last visited July 16, 2018), https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_with-markup.pdf.

[16] *Multistakeholder Process: Cybersecurity Vulnerabilities*, NAT. TELECOMM. & INFO. ADMIN. (last visited July 16, 2018), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[17] *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, U.S. COPYRIGHT OFFICE (last visited July 16, 2018), https://www.federalregister.gov/documents/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control#p-193; *Exemptions to Permit Circumvention of Access Controls on Copyrighted Works: Notice of Public Hearings*, U.S. COPYRIGHT OFFICE (last visited July 16, 2018), https://www.federalregister.gov/documents/2018/02/02/2018-02086/exemptions-to-permit-circumvention-of-access-controls-on-copyrighted-works-notice-of-public-hearings.

[18] *Known Disclosure Programs*, I AM THE CAVALRY (last visited July 16, 2018), https://www.iamthecavalry.org/resources/disclosure-programs/.

[19] *Id.*

[20] *Vulnerability Reporting*, AMAZON (last visited July 16, 2018), https://aws.amazon.com/security/vulnerability-reporting/; *Google Vulnerability Reward Program (VRP) Rules*, GOOGLE (last visited July 16, 2018), https://www.google.com/about/appsecurity/reward-program/; *Product Security at Intel*, INTEL (last visited July 16, 2018), https://www.intel.com/content/www/us/en/corporate-responsibility/product-security.html; *Coordinated Vulnerability Disclosure*, MICROSOFT (last visited July 16, 2018), https://technet.microsoft.com/en-us/security/dn467923.aspx.

[21] *Known Disclosure Programs*, I AM THE CAVALRY (last visited July 16, 2018), https://www.iamthecavalry.org/resources/disclosure-programs/.

As the number and diversity of organizations that have adopted CVD programs demonstrates, these programs are powerful, effective tools for helping manage cybersecurity risk. However, while the adoption of CVD programs and the frequency of CVDs has continued to climb, and the benefits have continued to grow, there remains resistance and challenges to its widespread adoption.

Part III – Challenges and Opportunities in Continued CVD Adoption

Legal Uncertainty

One of the primary challenges to CVD remains the uncertain legal environment in which CVD programs and participants must operate. Though numerous federal agencies now either operate CVD programs themselves or recommend CVD programs to their stakeholders, and though the PTO has issued specific civil liability carve-outs for certain types of good-faith vulnerability research, there still exists significant uncertainty regarding the legal differences between the types of research that typically inform CVD programs and "hacking." Consequently, a third-party who performs good-faith vulnerability research consistent with accepted CVD practices may nonetheless find themselves facing civil or criminal liability depending upon a given company's response.

For example, in a recent case, a well-known vulnerability researcher associated with Google's Project Zero—a team of researchers dedicated to finding cybersecurity vulnerabilities—discovered a bug in a company's product and reported it to the company in accordance with Project Zero's established procedures.[22] Following the company's issuance of a fix, Project Zero published details of the flaw, the researcher discussed the vulnerability in a public forum, and a reporter wrote an article covering the process.[23] Subsequently, the company sued both the reporter and the reporter's publication, alleging that the article made "false and misleading statements" regarding the nature of the vulnerability.[24]

While a public outcry ensued, and the company ultimately dropped the lawsuit and established a "bug bounty" program, the case has negatively impacted attitudes towards CVD.[25] One prominent cybersecurity expert, for example, stated publicly that "[they] know of at least

[22] *Chromium Bug Tracker – keeper: privileged ui injected into pages (again)*, PROJECT ZERO (last updated Dec. 17, 2017), https://bugs.chromium.org/p/project-zero/issues/detail?id=1481&desc=2#maincol.

[23] Dan Goodin, *For 8 days Windows offered a preloaded password manager with a plugin vulnerability*, ARSTECHNICA (Dec. 15, 2017), https://arstechnica.com/information-technology/2017/12/for-8-days-windows-offered-a-preloaded-password-manager-with-a-plugin-vulnerability/.

[24] *Keeper Security v. Dan Goodin*, No.17-cv-9117 (D. Ill. filed Dec. 17, 2017), https://www.documentcloud.org/documents/4333677-Keeper-Security-Inc-v-Goodin-et-al.html.

[25] Rob Wright, *Keeper Security forms vulnerability disclosure program with Bugcrowd*, TECHTARGET (Apr. 20, 2018), https://searchsecurity.techtarget.com/news/252439690/Keeper-Security-forms-vulnerability-disclosure-program-with-Bugcrowd; Zack Whittaker, *Security firm Keeper sues news reporter over vulnerability story*, ZDNET (Dec. 20, 2017), https://www.zdnet.com/article/security-firm-keeper-sues-news-reporter-over-vulnerability-story/; Keeper Security (@keepersecurity), TWITTER (Mar. 30, 2018, 1:01 PM), https://twitter.com/keepersecurity/status/979810981504266240.

two vulnerabilities in [the company's product]. Researchers are so intimidated by that company's legal threats that they don't publish or even disclose to them."[26]

Other recent examples further demonstrate this legal uncertainty and its consequences. Several additional security researchers and reporters have faced or are still facing legal threats.[27] A teen in Canada was charged with "unauthorized access of a computer" for downloading publicly-available documents from a misconfigured website.[28] Commentators argued that a state law in Georgia meant to combat computer crimes, which was passed by the legislature but ultimately vetoed by the Georgia governor after significant pushback, would have instead criminalized good-faith cybersecurity research.[29]

Each of these situations exacerbates the legal uncertainty in which CVD programs and participants must operate, and typically have the unfortunate effect of chilling both the willingness of companies to establish CVD programs and the willingness of participants to share valuable vulnerability information. With the exponential growth in the interconnection of society and the complexity that goes with it, such chilling effects on CVD post a serious threat to an otherwise effective and collaborative method to address cybersecurity risks.

Negative Public Responses

On the other end of the spectrum, a newer and relatively unexpected consequence has begun affecting companies with robust CVD programs; the public response to these companies performing CVDs has, in some cases, been negative. While the exact nature of these negative public responses varies, several recurring themes have arisen in Committee staff conversations with affected companies, including: news coverage with alarming or otherwise exaggerated headlines, which often suggest the companies do not take cybersecurity seriously; sales representatives using a competitors' CVDs to claim that the competitors' products are less secure than the ones the representative is trying to sell; and less "cybersecurity aware" customers who may take CVDs as signs that a company's products are "insecure," rather than recognizing that CVDs are a sign of a company's cybersecurity maturity.[30]

In other words, companies experiencing this kind of backlash to their CVDs are being punished for "doing the right thing." Further, this backlash is having additional, secondary effects. In some affected companies, it is causing officials to reconsider the value of and their

[26] Matthew Green (@matthew_d_green), TWITTER (Apr. 18, 2018, 5:38 PM), https://twitter.com/matthew_d_green/status/986765837750054913.

[27] Zack Whittaker, *Lawsuits threaten infosec research — just when we need it most*, ZDNET (Feb. 19, 2018), https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/.

[28] Jack Julian, *Teen charged in Nova Scotia government breach says he had 'no malicious intent'* CBC NEWS (Apr. 16, 2018), http://www.cbc.ca/news/canada/nova-scotia/freedom-of-information-request-privacy-breach-teen-speaks-out-1.4621970.

[29] Tasnim Shamma, *Ga. Senate Passes Bill Criminalizing 'Unauthorized Computer Access'* WABE (Feb. 15, 2018), https://www.wabe.org/ga-senate-passes-bill-criminalizing-unauthorized-computer-access/; J.M. Porup, *Georgia governor vetoes bill that would criminalize good-faith security research, permit vigilante action*, CSO (May 8, 2018), https://www.csoonline.com/article/3269206/legal/new-georgia-law-criminalizes-good-faith-security-research-permits-vigilante-action.html.

[30] Committee staff conversations with CVD stakeholders.

commitment to CVD.[31] For other companies that may be considering, but have not yet officially adopted, CVD programs, such negative responses discourage their doing so.

These types of negative public responses to CVDs and CVD programs risk derailing much of the progress that the federal government, the private sector, and third-party researchers have made over the past several years in improving society's overall cybersecurity. By discouraging the adoption of or continued investment in CVD programs, this backlash against CVD could encourage organizations to once again try to handle cybersecurity threats internally, rather than collaboratively. And as previously outlined, such a strategy is both woefully outdated and often ineffective.

Part IV – The Committee's Recommendations and Conclusion

As the past several years have shown, CVD is not just a valuable and effective tool for managing cybersecurity risk; the continued exponential growth of connected technologies and the complexity that such growth entails make it a necessity. Organizations in both the public and private sectors should follow in the footsteps of the agencies, departments, and companies highlighted here and adopt CVD programs as a critical component of their cybersecurity risk management strategies. To aid in that goal, the Committee offers two recommendations.

- First, Congress should explore ways to clarify the differences between "hacking" and CVD practices, to incentivize organizations to adopt CVD programs, and to offer protections to CVD participants who perform CVDs in accordance with modern best practices. In doing so, Congress could provide much needed legal certainty to CVD programs and participants, and thus encourage more organizations and third-parties to leverage CVD and its attendant benefits.

- Second, Congress should explore ways to encourage federal agencies and private sector stakeholders to address and minimize the negative public responses to CVDs. While the offering of legal certainty through the Committee's first recommendation would likely be the most powerful method through which to accomplish this goal, other strategies exist. For example, both organizational and customer education could combat the spread or entrenchment of misconceptions around CVD. Similarly, federal agencies may be able to help through their continued recommendation of and advocacy for CVD and the value it provides.

The growth of the Internet and connected technologies comes with an inescapable increase in the complexity and vulnerability of modern systems. These risks are shared across all facets and sectors of society, and no one organization is truly capable of managing these risks on its own. The nature of our modern connected society requires collaboration, and thus—as recent years have manifestly demonstrated—CVD remains one of the most valuable, effective methods for embracing that collaboration and facing those risks. Consequently, Congress, the rest of the federal government, the private sector, and third-parties should all find ways to support and adopt CVD.

[31] *Id.*