RAPID7

Comments to "Information on Current and Future States of Cybersecurity in the Digital Economy"

Docket Number: 160725650-6650-01

Sep. 9, 2016

Rapid7 submits these comments in response to the President's Commission for Enhancing National Cybersecurity's (CENC) request for public input on "Current and Future States of Cybersecurity in the Digital Economy."[1]

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks.

The modern world is increasingly dependent on the reliable flow of digital information. Cybersecurity failures – whether through cyber attack, technical malfunction or other means – are a serious risk to consumers, national security, and economic growth. Identifying and addressing the vulnerabilities inherent in technical systems is a critical measure in mitigating cyber threats, reducing opportunities for attackers, and diminishing risks of harm to the victims of a security breach.

Rapid7 strongly urges sustained leadership and investment in strengthening cybersecurity. We applaud this Commission and the Obama Administration for prioritizing cybersecurity, and we urge subsequent administrations to commit to making more sweeping progress. We believe the Administration's Cybersecurity National Action Plan,[2] the 2013 Executive Order for Improving Critical Infrastructure Cybersecurity,[3] and the NIST Framework for Improving Critical Infrastructure Cybersecurity,[4] and other initiatives establish a good foundation, and we urge Congress and the Administration to continue collaborating to thoughtfully implement, fund, and promote consistent

---

[1] President's Commission for Enhancing National Cybersecurity, Notice, Request for information, *Information on Current and Future States of Cybersecurity in the Digital Economy*, 81 FR 52827, Aug. 10, 2016, https://federalregister.gov/a/2016-18948.

[2] Fact Sheet: Cybersecurity National Action Plan, White House, Feb. 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[3] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, White House, Feb. 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[4] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, Feb. 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

industry participation in these efforts. There is still a long way to go before U.S. cybersecurity is commensurate with today's ever-evolving threat landscape.

I. Critical Infrastructure Cybersecurity

A. Address known vulnerabilities through secure design and patching

Cybersecurity of critical infrastructure – including national energy, health, financial, and communications systems – is both highly important and challenging. The government and private sectors must make strategic investments in security based on risk assessments accounting for the potential severity of harm and probability of occurrence. No system will be made perfectly secure, but several steps can be taken now to address critical security flaws.

An area of immediate focus should be to defend against known vulnerabilities in applications and operating systems. Many attackers, both sophisticated and unsophisticated, leverage security flaws that are publicly known, but which a target has not sufficiently remediated or mitigated.[5] For example, it is not uncommon to see systems with hardcoded, default, or public passwords connected to the internet. Finding and strengthening these passwords, and ideally adding multi-factor authentication requirements (see Section V, below), should be a priority for critical infrastructure.

A common issue with critical infrastructure systems is that the underlying software was often designed before widespread internet adoption, and is now integrated with internet functionality it was not originally intended to have. The process of securing critical infrastructure should begin with integrating security principles into systems at the design stage to avoid known flaws and reduce attack surface.[6] "Secure by design" approaches should include transparency and coordination of critical infrastructure supply chains (see also Section IV(B), below). Post-market, periodic penetration testing and patching of products, applications, and operating systems are crucial because the catalog of known vulnerabilities is always evolving. Compliance with baseline security standards alone is unlikely to be sufficient.[7]

These practices should not be – and are not – limited to critical infrastructure systems. Ideally, non-critical functions should be segmented from critical components, but this is not always achievable.

---

[5] 2016 Data Breach Investigations Report, Verizon, pg. 15, http://www.verizonenterprise.com/verizon-http://verizonenterprise.com%2Fresources%2Freports%2Frp_DBIR_2016_Report_en_xg.pdf&usg=AFQjCNGO_-X9afKczCQUHfqqfh1pOSeA0g (last accessed Sep. 6, 2016). See also Security Threat Landscape Still Plagued by Known Issues, says HP, HP, Feb. 23, 2015, http://www8.hp.com/us/en/hp-news/press-release.html?id=1915228.

[6] Ron Ross, Michael McEvilley, and Janet Carrier Oren, Systems Security Engineering, NIST Special Publication 800-160, National Institute of Standards and Technology, May 2016, http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf.

[7] Teri Radichel, *Case Study: Critical Controls that Could Have Prevented Target Breach*, SANS Institute Reading Room, Aug. 5, 2015, pg. 7, https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

Cybersecurity flaws in periphery or support systems that are connected to critical infrastructure present risks, as attackers can leverage those flaws to penetrate critical infrastructure that may otherwise be relatively secure. To the extent feasible, risk assessment and vulnerability remediation and mitigation should be holistic across assets.[8]

Recommendation summary:

- Focus initially on the most common and severe known vulnerabilities for a given sector.
- Design securely, including across the supply chain, to reduce attack surface and avoid known vulnerabilities.
- Implement a regular testing and patching regime for known vulnerabilities.
- Segment critical and non-critical systems.
- Ensure systems connected to critical infrastructure are included in assessment, remediation, and mitigation efforts.

B. Protect strong encryption

Encryption is a fundamental means of protecting data from unauthorized access or use. Critical infrastructure, commerce, government, and individual internet users already depend on strong security for communications, and this reliance on encryption will only continue to grow as more of the world is digitized. Weak transport security, unencrypted storage, and faulty authentication are common vulnerabilities Rapid7 has encountered in its research and practice. To protect against these and other cybersecurity flaws, Rapid7 believes companies and innovators should be able to use the encryption protocols that best protect their customers and fit their service model – whether that protocol is end-to-end encryption or some other system.

However, because strong encryption can pose challenges to law enforcement access to data, some policymakers have called for regulations that would forbid the use of encryption without providing a special means of access to data, such as an encryption "backdoor" or custom software that removes product security features.[9] While we do not find fault with law enforcement agencies attempting to execute valid search or surveillance orders, proposals to undermine encryption would incur broad negative implications for cybersecurity by creating new breach risks and attack surfaces for cybercriminals.[10]

Repeatedly, government officials have suggested establishing a legal requirement that companies weaken encryption by creating a means of "exceptional access" to software and communications

---

[8] *Id.*, pgs. 5-6.
[9] See, e.g., Sen. Dianne Feinstein, *Intelligence Committee Leaders Release Discussion Draft of Encryption Bill*, Apr. 13, 2016, http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649.
[10] Harley Geiger, *Security vs. Security, Rapid7 supports strong encryption*, Mar. 31, 2016, https://community.rapid7.com/community/infosec/blog/2016/04/01/security-vs-security-rapid7-supports-strong-encryption.

services that government agencies can use to unlock encrypted data.[11] This option would impose significant security risks for the underlying software or service by creating attack surfaces for bad actors, including cybercriminals and unfriendly international governments.[12] The huge diversity of modern communications platforms and software architecture makes it impossible to implement a one-size-fits-all backdoor into encryption. Instead, to comply with a hypothetical mandate to weaken encryption, different companies are likely to build different types of exceptional access. Some encryption backdoors will be inherently more or less secure than others due to technical considerations, the availability of company resources to defend the backdoor against insider and external threats, the attractiveness of client data to bad actors, and other factors. The resulting environment would most likely be highly complex, vulnerable to misuse, and burdensome to businesses and innovators.

Rapid7 also shares concerns that requiring U.S. companies to provide exceptional access to encrypted communications for U.S. government agencies would lead to sustained pressure from many jurisdictions – both local and worldwide – for similar access. Companies or oversight bodies may face significant challenges in accurately tracking when, by whom, and under what circumstances client data is accessed – especially if governments have unmediated access to decryption keys. If U.S. products are designed to be inherently insecure and "surveillance-ready," then U.S. companies will likely face a considerable competitive disadvantage in international markets where more secure products are available.

Legal mandates to weaken encryption are unlikely to keep unbreakable encryption out of the hands of well-resourced criminals or terrorists. Open source software is commonly "forked," or independently modified into a distinct version, and it should be expected that developers will modify open source software to remove an encryption backdoor.[13] Jurisdictions *without* an exceptional access requirement could still distribute closed source encryption software without a backdoor on the global market.[14] As a result, the cybersecurity risks of weakened encryption are especially likely to fall on users who are not already security-conscious enough to seek out these workarounds.

Intentionally weakening encryption or other technical protections would ultimately undermine the security of the end-users, businesses, and governments. Creating secure software is quite difficult under the best of circumstances, and forcing developers to actively undermine their own security features would undo decades of security learnings and practice. From Rapid7's perspective, the best path forward is that which would provide the best security for the highest number of well-meaning

---

[11] James Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Federal Bureau of Investigation, Oct. 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
[12] Abelson et al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, Jul. 6, 2015, pg. 15, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf#page=17.
[13] Ryan Paul, *Oracle gives up on OpenOffice after community forks the project*, Ars Technica, Apr. 17, 2011, http://arstechnica.com/information-technology/2011/04/oracle-gives-up-on-ooo-after-community-forks-the-project.
[14] Schneier, Seidel, and Vijayakumar, *Worldwide Survey of Encryption Products*, Feb. 11, 2016, https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

individuals. We want the government to help prevent crime by working with the private sector to make communications services, commercial products, and critical infrastructure more trustworthy and resistant to cyber attack. To that end, Rapid7 urges the Commission to openly embrace greater use of strong encryption free of legal mandates that compel companies and innovators to undermine their security. The foundation of greater cybersecurity will benefit us all in the future.

Recommendation summary:

- Urge against legal mandates requiring exceptional access to encrypted data.
- Support the use of strong encryption among private and public sector actors.

II. Cybersecurity Workforce

A. Leverage independent security research

The U.S. has long faced a workforce shortfall for cybersecurity professionals. The Executive Branch initiatives to bolster the federal cybersecurity workforce are welcome and needed,[15] though national demand is expected to exceed supply for years to come.[16] To meet the greater need for security as digital goods and services are more widely deployed, the U.S. should consider ways to leverage independent security researchers as a decentralized talent pool.

Independent security researchers access software and computers to identify and assess security vulnerabilities. This may refer to users or administrators who uncover issues incidentally or accidentally, or security professionals who intentionally test systems to identify problems, and raise awareness to vendors and users so the issue is resolved. This research strengthens cybersecurity and helps protect consumers because the researchers call attention to vulnerabilities that manufacturers may have missed or ignored, which encourages manufacturers or other parties to make the appropriate fixes or mitigations to keep people safe. Independent security research will grow in importance to cybersecurity as the quantity and variety of connected devices will prevent manufacturers and operators alone from catching all vulnerabilities without independent expertise and manpower, and consumers are less likely to take steps themselves to effectively secure flawed devices.

As compared to several years ago, policymakers more frequently recognize the value of independent security research. For example, in Oct. 2015, the U.S. Copyright Office approved a temporary

[15] Shaun Donovan et al., *Strengthening the Federal Cybersecurity Workforce*, White House, Jul. 12, 2016, https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce.
[16] Steve Morgan, *Cybersecurity job market to suffer severe workforce shortage*, CSO, Jul. 28, 2016, http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html.

exemption to Sec. 1201 of the DMCA for security research.[17] Another example: In April 2016, the state of Washington enacted the Washington Cybercrime Act to revise the state's computer crime laws, including helpful exceptions for white hat security researchers.[18]

However, several existing laws chill security research, which can hinder independent efforts to assess the security of IoT devices. The Computer Fraud and Abuse Act (CFAA), Section 1201 of the Digital Millennium Copyright Act (DMCA), and other laws contain broad prohibitions on independent access to computers and software without distinguishing between malicious attackers and individuals that seek to enhance cybersecurity.[19] Although we recognize the beneficial role of these laws in deterring cybercrime, balancing greater flexibility for researchers and innovators with law enforcement needs is increasingly important.

In addition, some federal and state legislative proposals would impose broad and redundant restrictions on independent access to software that would hinder researchers and independent repair services that can assess and fix the devices' cybersecurity vulnerabilities. For example, in Oct. 2015, a House Energy and Commerce Subcommittee released draft legislation that would have levied heavy fines on anyone accessing a car's software without authorization for any reason – regardless of whether the accessor purchased the car, or if the car was accessed for cybersecurity research purposes.[20] Similarly, a bill restricting access to vehicle software was introduced in the Michigan Senate.[21] While safety is certainly an important consideration, new computer crime laws should not undermine cybersecurity by imposing blanket access and use restrictions that further chill independent research and repair.

Leveraging beneficial independent research to bolster U.S. cybersecurity efforts will require reevaluation of regulatory and policy roadblocks to safely performing security research and disseminating the results to prompt a correction. Independent review of software for security vulnerabilities does not seek to infringe IP rights, destroy property, or endanger safety, but cybersecurity and transparency are undermined by regulations that chill standard independent research practice. Rapid7 urges the Commission to work with federal and state agencies and legislatures to ensure new regulations on access and use to computers and software do not unduly restrict independent research and repair of cybersecurity vulnerabilities.

---

[17] Jen Ellis, *New DMCA Exemption is a Positive Step for Security Researchers*, Rapid7, Oct. 28, 2015, https://community.rapid7.com/community/infosec/blog/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers.
[18] Washington (state) legislature, H.B. 2375 - 2015-16, Sec. 3(10)-(11). Signed into law Apr. 1, 2016. Available at http://app.leg.wa.gov/billinfo/summary.aspx?year=2015&bill=2375.
[19] Deirdre Mulligan, Nick Doty, and Jim Dempsey, *Cybersecurity Research: Addressing the Legal Barriers and Disincentives*, Berkeley Center for Law and Technology, Sep. 28, 2015, http://ondoc.logand.com/d/5689/pdf.
[20] Harley Geiger, *Draft Car Safety Bill Goes In The Wrong Direction*, Center for Democracy & Technology, Oct. 20, 2015, https://cdt.org/blog/draft-car-safety-bill-goes-in-the-wrong-direction.
[21] Michigan (state) senate, S.B. 0927, Sec. 4(2), Apr. 28, 2016, https://www.legislature.mi.gov/documents/2015-2016/billintroduced/Senate/pdf/2016-SIB-0927.pdf.

Recommendation summary:

- Leverage expertise and manpower of independent security researchers to help overcome cybersecurity workforce shortfall.
- Advise against new regulations that place overbroad restrictions on access to computers and software.
- Support balanced legal reforms and policies that enable responsible independent cybersecurity research.

III. Public Awareness and Education

A. Encourage adoption of vulnerability disclosure and handling policies

Since cybersecurity vulnerabilities cannot be completely eliminated pre-market, organizations must be prepared to discover, assess, and remediate cybersecurity flaws throughout the product lifecycle. As the growth of digital goods and services – including the proliferation of Internet of Things devices – enlarges the attack surface for malicious actors, security vulnerabilities may be too voluminous or difficult to find for many software vendors alone. It is increasingly crucial to foster an environment where vendors take disclosure of security issues from external sources – such as independent security researchers – seriously and openly, rather than with legal threats or avoidance. To do this effectively, it is critical for organizations to have a plan and policy in place to receive and process vulnerability information from external sources, such as independent security researchers.

Rapid7 believes government agencies, businesses, and consumers benefit most when software vendors collaborate with researchers to address cybersecurity vulnerabilities. Having a vulnerability management and disclosure process in place can help companies quickly address vulnerabilities disclosed to them by external sources. Such processes can also help protect researchers by providing them with a clear means to communicate and reducing the risk of conflict or misunderstanding between researchers and vendors.

Best practices for vulnerability disclosure and handling do exist,[22] and businesses and government agencies are increasingly implementing coordinated vulnerability disclosure policies.[23] However, adoption of flexible and mature processes for handling unsolicited vulnerability reports is not yet the norm. Rapid7 has witnessed a wide range of responses in our experience researching and disclosing cybersecurity flaws to vendors; some vendors were impossible to contact, others did not respond,

---

[22] ISO/IEC 29147:2014, Information Technology – Security Techniques – Vulnerability Disclosure, International Standards Organization, Feb. 15, 2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170. ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling, International Standards Organization, Nov. 1, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[23] *See* Sean Gallagher, *GM embraces white-hat hackers with public vulnerability disclosure program*, Ars Technica, Jan. 8, 2016, http://arstechnica.com/security/2016/01/gm-embraces-white-hats-with-public-vulnerability-disclosure-program. *See also* Dept. of Defense, *Statement by Pentagon Press Secretary Peter Cook on DoD's Partnership with HackerOne on the "Hack the Pentagon" Security Initiative*, Mar. 31, 2016, http://www.defense.gov/News/News-Releases/News-Release-View/Article/709818/statement-by-pentagon-press-secretary-peter-cook-on-dods-partnership-with-hacke.

while still others had an established process for handling incoming product vulnerabilities and worked closely both with us and upstream vendors to remediate the flaw. Unfortunately, the latter group has traditionally been by far the smallest, though this is slowly starting to improve.

We urge the Commission to support increased education about the value of adhering to a clear process for vulnerability disclosure and handling. This effort should aim to grow awareness among both vendors (including manufacturers, developers, and service providers in the public and private sectors) and security researchers (including professionals and accidental discoverers). The Dept. of Commerce's multistakeholder process on vulnerability disclosure, which Rapid7 supports, has already laid good groundwork for this engagement, but promoting broad adoption and effective implementation will require a long-term project.[24]

Recommendation summary:

- Work with public and private sector entities to adopt processes to receive and handle vulnerabilities disclosed by external sources.
- Urge security researchers to adopt coordinated disclosure policies to minimize misunderstandings and maximize the likelihood of appropriate corrective action.
- Support efforts to educate vendors and researchers regarding vulnerability disclosure and handling policies.

IV. Internet of Things (IoT)

A. Improve IoT update practices

IoT devices are general purpose, networked computers running relatively complex network-capable software.[25] It is widely accepted that such software ships with exploitable bugs and implementation-based exposures. Add in external components and dependencies – such as cloud-based controllers and programming interfaces, the surrounding network, and other externalities – and vulnerabilities and exposures are all but guaranteed. IoT is typically composed of multiple interactive components like hardware, software, firmware, and cloud technologies, requiring consideration of how the security of each individual component can affect the security of the other components. Since IoT devices are highly diversified and include very inexpensive items manufactured by companies with limited security experience, the result can be a considerably more exploitable environment than the status quo.[26] Because IoT devices tend to interact directly with physical objects and infrastructure, the risks of

[24] Multistakeholder Process: Cybersecurity Vulnerabilities, National Telecommunications and Information Administration, Apr. 08, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[25] Deral Heiland, *What Is the Internet of Things? The Current Struggle With Defining IoT*, Rapid7, Jun. 16, 2016, https://community.rapid7.com/community/infosec/blog/2016/06/27/what-is-the-internet-of-things-the-current-struggle-with-the-definition-of-iot.

[26] Ashkan Soltani, *What's the security shelf-life of IoT?*, Federal Trade Commission, Feb. 10, 2015, https://www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-life-iot?utm_source=govdelivery.

physical danger posed by cybersecurity flaws in some devices can be greater than that for purely digital applications.

Today, a commonly accepted way to effect a rapid rollout of patches for IoT devices simply does not exist. IoT devices, unlike traditional computers, often lack an effective update and upgrade path once the devices leave the manufacturer's warehouse. Without a patching capability, it is difficult to correct devices' known security flaws at a large scale. As a result of the growth of IoT, unpatchable IoT devices are coming online at an unprecedented rate,[27] creating a wave of unsecurable-after-the-fact devices. Although we are optimistic that patchable IoT devices will become more common, unpatchable legacy devices will likely linger on the market for some time.

One factor that should be considered is that many manufacturers entering the IoT space traditionally work with development processes and timeframes that are vastly different to those typically associated with software or cloud services development cycles. For example, many cloud services work in essentially continuous develop-and-deploy cycles that see updates made to the service on a weekly, or even daily, basis. In comparison, manufacturing new versions of cars or medical devices may take years. It is challenging for drawn out processes to incorporate quick response practices for vulnerability handling and patching, yet doing so is critical given the potential risks of inaction.

Another factor to consider is that companies may not plan to provide long-term security support for lower-end, commodity IoT devices with thin profit margins. Nonetheless, we believe companies should make plans to maintain some patching capability beyond the typical lifetime or planned obsolescence of a product, such as by authorizing third parties to issue patches after a certain period. This will help protect end-users that rely on IoT devices and systems after the vendor ceases to provide security support.

Rapid7 urges the Commission to encourage industry to implement an update management program for IoT. Rapid7 generally views security update and advisory mechanisms as a mandatory component of device or software cybersecurity plans. We also do not believe the technical challenges to updating IoT devices are insurmountable at present. Effective patching is challenging even for mature market sectors such as smartphones and routers, but those sectors nonetheless have update mechanisms.[28] Because connectivity may be new to many product categories (e.g., a toaster versus a connected toaster), many IoT companies may be relatively unfamiliar with the complex mechanics of update management, but we believe it is essential that updating becomes a more regularized and extensive practice for IoT.

Recommendation summary:

- Encourage IoT companies to implement field upgradability and patching processes to fix cybersecurity vulnerabilities in connected devices as rapidly as reasonably possible.

---

[27] Gartner estimates at least 20 billion connected devices in 2020. *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015*, Gartner, Nov. 10, 2015, http://www.gartner.com/newsroom/id/3165317.
[28] Liam Tung, *Google: Android Marshmallow on steady rise, unpatchable phones falling*, ZDNet, May 4, 2016, http://www.zdnet.com/article/google-android-marshmallow-on-steady-rise-unpatchable-phones-falling.

- Urge IoT companies to consider plans to sustain security support of IoT devices after the lifetime of the device.

B. Coordinate supply chain security and transparency

The devices being built and shipped today are establishing the status quo of how they will be designed, assembled, commoditized, and supported in the future. The IoT supply chain is quite complex, due in part to the diversity and interdependence of systems. This complexity risks a larger attack surface with undiscovered vulnerabilities, as well as greater challenges in tracking, recalling, and replacing flawed parts. We should take the opportunity, now, to bring clarity to the IoT supply chain, evaluate the vulnerabilities and exposures most common to these devices, and implement update management programs to work across the manufacturing process.

Rapid7 supports greater voluntary standardization and use of open source for IoT components as a means to more easily repair and replace vulnerable components. In addition, it would be valuable to establish a system or authority that can help researchers identify affected manufacturers and service providers, and assist with the disclosure, tracking, and remediation of vulnerabilities, and coordinate with relevant third parties both domestically and internationally. Today, CERT/CC does much of this, but we believe CERT/CC is in need of greater support and funding to build on these efforts.

Rapid7 would support an open model of collaboration with vendors and manufacturers to advance supply chain security and transparency. Ideally the model would adopt clear vulnerability disclosure and handling processes, incorporate as much automation as reasonably possible, and draw upon the National Institute of Standards and Technology's guidance on security for an organization's supply chain.[2] In the financial payments industry, which, like IoT, involves a complex ecosystem of many organizations, major credit card organizations formed the Payment Card Industry Security Standards Council and developed the Payment Card Industry Data Security Standard.[1] A modified version of this model may be helpful to coordinate security issues across the IoT supply chain.

Recommendation summary:

- Adopt greater standardization and use of open source for IoT device components.
- Enhance broad collaboration among IoT vendors, manufacturers, and researchers to strengthen security and transparency across the IoT supply chain.

V. Identity and Access Management

A. Encourage adoption of multi-factor authentication

As organizations' perimeter defenses grow more secure, widespread, and cost-effective to deploy, frontal assaults are becoming less economical to attackers in terms of cost, time, labor, and risk. However, the costs and risks of credential-based attacks are often lower by comparison, and more challenging to defend against. At present, unauthorized use of stolen, weak, and default credentials

contribute to a high proportion of data breaches, including targeted attacks and automated malware infections.[29]

There are a variety of ways to boost the strength of credentials, such as by using character requirements or password managers, although these alone tend not to work if the credentials are stolen or intercepted. In addition to these strategies, Rapid7 agrees with the President's Cybersecurity National Action Plan that wider use of multi-factor authentication may significantly improve the protection of sensitive or critical assets from credential-based attacks.[30] We urge the Commission to facilitate broader adoption of multi-factor authentication, including support for incorporating multi-factor authentication standards into the NIST Framework's Core.

There is legitimate concern that businesses and individuals won't embrace multi-factor authentication because the extra steps involved may be viewed as unwieldy. For this reason, we urge continued research and attention to developing methods of implementing multi-factor authentication with as little friction as possible to encourage consumer and enterprise adoption. The use of authentication apps, USB tokens, and privacy-respecting biometric readers on devices all hold potential in this regard. Even with the extra steps required, however, we believe multi-factor authentication should be considered a fundamental security tactic for environments holding or connected to critical or sensitive assets.

Recommendation summary:

- Urge greater adoption of multi-factor authentication to protect credentials, especially for critical systems.
- Expand research into developing several easy and cost-effective methods to implement and use multi-factor authentication.
- Promote research and public awareness initiatives that educate individuals on the benefits of multi-factor authentication for consumer services that contain personal information.
- Support integration of authentication standards in NIST Framework.

VI. Government handling of cybersecurity vulnerabilities

A. Vulnerability Equities Process

Rapid7 supports effective law enforcement and recognizes that investigation approaches and techniques must evolve to match the nature of commerce, property, and crime – all of which have changed in the Information Age. It is not an irrational priority for law enforcement and national security agencies to modernize their computer penetration capabilities to be commensurate with new

[29] 2016 Data Breach Investigations Report, Verizon, pg. 24, http://www.verizonenterprise.com/verizon-http://verizonenterprise.com%2Fresources%2Freports%2Frp_DBIR_2016_Report_en_xg.pdf&usg=AFQjCNGO_-X9afKczCQUHfqqfh1pOSeA0g (last accessed Sep. 6, 2016).
[30] Fact Sheet: Cybersecurity National Action Plan, White House, Feb. 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

technologies and savvy adversaries. A higher level of hacking and digital forensic expertise for law enforcement agencies should improve their ability to combat cybercriminals more generally. However, this approach raises important questions related to cybersecurity and transparency.

Offensive use of cybersecurity vulnerabilities – unlike more traditional data collection mechanisms, such as wiretaps – carry an expectation that hacking can result in system damage, degradation, or misuse. Vulnerabilities used by one government can be used by other governments or non-government adversaries. The longer that cybersecurity vulnerabilities in commercial products or infrastructure are not disclosed to the vendors and remain uncorrected, the longer the users of those products and infrastructure are at risk. Companies may face difficulty selling products, such as routers or messaging apps, that are believed to carry undisclosed cybersecurity vulnerabilities exploited by government agencies. Although Rapid7 certainly recognizes there are scenarios where it is prudent for the government to keep vulnerabilities classified, we believe the interests of cybersecurity are typically best served by government disclosure of vulnerabilities to companies for patching to the greatest extent reasonably possible.

At present, there appear to be few clear and publicly available standards for government use of vulnerabilities.[31] White House Cybersecurity Coordinator Michael Daniel noted there were "few hard and fast rules" for disclosing vulnerabilities, but pointed out that zero day stockpiles put Internet users at risk and would not be in the interests of national security.[32] The government's "vulnerabilities equities process" rightly weighs several important factors in considering whether to disclose or exploit cybersecurity vulnerabilities, but this process is not formalized in law and has a low level of transparency.[33]

Rapid7 urges the Commission to support formalizing the vulnerabilities equities process through Executive Order or legislation, requiring government-wide compliance, establishing minimum transparency standards regarding the high-level criteria used to weigh disclosure. The process should maintain a strong bias towards disclosure of vulnerabilities to vendors for patching, ideally establishing a regular workflow and data exchange between the government and companies through the process.

Recommendation summary:

- Formalize the vulnerabilities equities process in legislation or Executive Order.
- Set transparency standards for the criteria used to weigh disclosure of vulnerabilities to affected entities.
- Maintain a bias toward disclosure of vulnerabilities whenever feasible in the vulnerabilities equities process.

---

[31] Jonathan Mayer, *Constitutional Malware*, Sep. 4, 2016, available at SSRN: http://ssrn.com/abstract=2633247.
[32] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, White House, Apr. 28, 2014, https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.
[33] Ari Schwartz, Rob Knake, *Government's Role in Vulnerability Disclosure*, Harvard Kennedy School Belfer Center, Jun. 2016, http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.

* * *

We appreciate the opportunity to share our views. If there are additional questions, or if Rapid7 can provide any further assistance, please contact Harley Geiger, Director of Public Policy, at Harley_Geiger[at]Rapid7.com. Thank you.

END