Free markets. Real solutions.

R STREET POLICY STUDY NO. 86
February 2017

ALIGNING CYBERSECURITY INCENTIVES IN AN INTERCONNECTED WORLD

Anne Hobson

CONTENTS

INTRODUCTION

In the stop-motion animated short "Wallace & Gromit: The Wrong Trousers," the protagonist Wallace's alarm clock kicks off a Rube Goldberg-like chain of machines and devices that dress him and make him breakfast. The so-called "internet of things" is set to make this sort of fiction a reality. Connected homes, appliances and infrastructure have the potential to make us more productive. Today, you can set your alarm clock remotely and have it signal your coffee maker to start and the water heater to get your shower ready.

The term "internet of things" dates to 1999, when the founders of the Massachusetts Institute of Technology's Auto-ID Labs began using it to describe a class of identification technologies used in automation processes.[1] The actual technologies are significantly older. It's believed the computer science department at Carnegie Mellon University programmed the first internet-connected device—a Coca-Cola vending machine—in the mid-1970s.[2] As the story goes, the department installed microswitches to sense whether bottles were present in the machine, with that information relayed to a server that students could access from anywhere on the internet.

Though the term has been with us nearly two decades, there remains significant disagreement about what, precisely, the "internet of things" describes. Since its inception, it has been used alternatively to include or exclude various classes of connected objects. Key to its global spread was a 2005 report by the United Nations' International Telecommunication Union that characterized the internet of things as "ubiquitous computing," complete with machine-to-machine communication and real-time connectivity.[3] In the United States, the Federal Trade Commission has adopted a definition that hinges on whether or not a given class of objects traditionally had embedded computing power; networked appliances and thermostats thus qualify as internet-of-things devices, but computers, tablets and smartphones do not.[4] The management consultant McKinsey & Co. employs a definition that also excludes computers and smartphone apps, on grounds that they are designed to receive intentional human input.[5] The Institute of Electrical and Electronics Engineers defined the internet of things as "a network of items—each embedded

1. Gérald Santucci, "The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects," European Commission, 2010. https://pdfs.semanticscholar.org/adb7/03eb4c53ccba53a8973fbff2f30563363a58.pdf

2. Carnegie Mellon University Computer Science Department, "The Only Coke Machine on the Internet," https://www.cs.cmu.edu/~coke/history_long.txt

3. International Telecommunication Union, "The Internet of Things," *ITU Internet Reports*, 2005. https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

4. Federal Trade Commission, "Internet of Things: Privacy and Security in a Connected World," FTC Staff Report, January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

5. James Manyika, et al., "Unlocking the Potential of the Internet of Things," *McKinsey Global Institute*, June 2015. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

with sensors—which are connected to the internet."[6] The U.S. Commerce Department's National Institute of Standards and Technology (NIST)—recognizing there is no universally agreed-upon definition—defines internet-of-things devices by the presence of certain behavioral features: a sensing function, an aggregating function, a communications channel and a decision trigger.[7]

For the purposes of this paper, we use the term "internet of things" to refer to an array of connected objects with unique identifiers that have the ability to transfer data over a network. The internet of things consists of a variety of network-enabled physical objects, including appliances, objects using near-field communications, machine components, sensors, endpoints, wearables, computers and phones. That being said, we recognize that objects that are tagged with unique identifiers, but are not "smart," in that they do not have the ability to both send and receive data, present less cybersecurity risk. Conflating these things into one category can be problematic. Our definition approximates the category of objects included in the internet-of-things issues that policymakers will likely face.

The internet of things holds promise for applications in the fields of transportation, infrastructure, agriculture, energy, manufacturing, health and communications, among others. McKinsey predicts that internet-of-things adoption worldwide could generate between $3.9 and $11.1 trillion per year by 2025, equivalent to up to 11 percent of the global economy.[8] Internet-of-things devices can help monitor chronic conditions, such as diabetes. Smart homes made up of networked appliances can help to streamline routines and chores. Smart cities composed of networked infrastructure can smooth traffic flows and allocate energy more efficiently. Sensor-laden trash cans can signal when they need to be emptied, while sensors in bridges and roads can signal the need for repair.

For all the amazing potential of the internet of things to be realized, systems need to anticipate and design against vulnerabilities. The most common of these is a cyber-attack, a malicious attempt to access, damage or disrupt information or systems. To fend off potential attacks, internet-of-things devices and systems need to be equipped with appropriate cybersecurity defenses, which are designed to protect information systems from criminals, nation-states and unauthorized users.

Different aspects of connected devices pose different kinds and degrees of cybersecurity risk, with the internet-enabled features being the root source of most concerns. For example, there are privacy and surveillance implications associated with identifying technologies like RFID, as well as with "always-on" sensing capabilities.[9] Devices that interact directly with the physical world or that have clear real-world consequences can result in safety issues, as was seen in the recent hacks of the Ukrainian power grid.[10]

Because of the nature of network effects, internet-of-things devices present a unique problem to the internet as a whole. When devices are connected, one device's vulnerability becomes a problem for the entire network. This is not a new threat, as networked devices have been around since the 1960s. However, the scale of interconnection among today's devices magnifies the consequences of insecurity. Common vulnerabilities include insecure network services, software and firmware; insecure security configurability and authentication, authorization and verification systems; and insecure cloud, mobile and web interfaces.

The insecurity of the internet of things has helped to create the equivalent of an active warzone. Compromised devices can be organized into "botnets" that are used to disrupt internet service broadly in what are known as distributed denial of service (DDoS) attacks. Large-scale internet outages due to denial of service attacks are increasing in number and frequency.[11] Other types of internet-of-things-based attacks include physical attacks, reconnaissance attacks, access attacks and attacks on privacy, including data-mining, cyber espionage and eavesdropping, as well as tracking and password-based attacks.[12]

A massive Oct. 21, 2016 cyber-attack rendered popular sites such as CNN, Twitter and Netflix inaccessible worldwide.[13] That event prompted the U.S. House Committee on Energy and Commerce to convene hearings to understand the role

6. Roberto Minerva, Abyi Biru, and Domenico Rotondi, "Towards a Definition of the Internet of Things," IEEE Internet Initiative, May 2015. http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

7. Jeffrey Voas, "Network of 'Things'," NIST Special Publication 800-183, July 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

8. Manyika, 2015.

9. Gilad Rosner, *Privacy and the Internet of Things: Challenges and risks of connected devices*, O'Reilly Media, 2017. http://www.oreilly.com/iot/free/privacy-and-the-internet-of-things.html

10. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

11. Arbor Networks, "Worldwide Infrastructure Security Report," 11: 1-115, 2016. https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

12. Mohamed Abomhara and Geir M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security*, Vol. 4, pp. 65-88, May 22, 2015. http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf

13. Sara Ashley O'Brien, "Widespread Cyberattack Takes Down Sites Worldwide," CNN Money, Oct. 21, 2016. http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/

of connected devices in the internet disruption.[14] The outage was also at least partially responsible for the National Institute of Standards and Technology moving up the release date of the final draft of planned guidance to provide cybersecurity and mitigation resources for internet-of-things manufacturers.[15]

The pace of progress in creating effective cybersecurity protocols currently lags the speed with which internet-of-things systems are developing, but this does not always have to be the case. The risk of cyber-attack is becoming both more costly and more visible. Companies do not want the reputation or brand damage associated with selling insecure devices. As one recent example illustrates, the company responsible for the vulnerable webcams leveraged in the October 2016 Mirai botnet chose voluntarily to recall millions of devices.[16] Insecure internet-of-things devices cause negative externalities, as one individual's use of a vulnerable product can reduce the well-being of others within the network. Bruce Schneier—a fellow at Harvard University's Berkman Klein Center for Internet & Society—is among the prominent voices calling for government to intervene to correct this "market failure."[17]

However, if we turn Schneier's logic on its head, market failures can become market opportunities.[18] In other words, the absence of security is an opportunity for entrepreneurs to sell secure internet-of-things devices, make security cheaper to implement and to broker information about device security. Users currently are largely unaware of the negative effects of their insecure devices and companies are often unaware of vulnerabilities in their devices. Such information asymmetries offer opportunities for strong private mechanisms to evolve. Third-party accreditation organizations, standards organizations and ratings bodies can provide information to consumers about their products' security, just as the nonprofit Underwriters Laboratories certifies safe products with their "UL" mark.

Cyber insurance also can help the market to manage and transfer risk, and to internalize the negative externality through risk-based insurance premiums. Through the processes of cyber-insurance underwriting and ratemaking, manufacturers are offered incentives to become aware of vulnerabilities. So long as insurers remain free to craft new products and charge appropriate risk-based prices, and efforts are not made to displace private coverage with some kind of government "backstop," the market for cyber insurance should continue to develop rapidly. The federal government could help encourage the burgeoning market by requiring that federal internet-of-things contractors use insurance or other risk-transfer mechanisms to take financial responsibility for cyber liabilities they may create for taxpayers.

Given the challenge posed by an insecure internet of things, policymakers must avoid the knee-jerk response to institute regulations that require certain prescribed device-security standards. Government is limited in its cyber-security expertise and local knowledge, particularly given the complexity and speed of technological development, which make it impossible for lawmakers and regulators to know what type of requirements to impose. Because devices have unique functions, protocols and uses, one-size-fits-all regulation based on design standards would set inadequate or overly complex standards in stone, not to mention introducing compliance costs that could deter internet-of-things innovation. Overly prescriptive regulations also could limit companies' flexibility to respond to issues as they arise.

Because of potential pitfalls in a federal regulatory approach to internet-of-things standards, identifying market-based solutions is critical. This paper explores two market-based mechanisms—cyber insurance and third-party accreditation—that could help secure the internet of things. It also examines the role policymakers can play in supporting broader adoption of cyber insurance coverage.

STATE OF THE INTERNET OF THINGS

Depending on whether traditional human-interfacing devices like computers and smartphones are included in the definition, there currently are between 6.4 billion and 17.6 billion internet-of-things devices globally.[19] To put this in perspective, the world's population is around 7.3 billion people.[20] Projections for the number of connected devices in 2020 range from an estimate of 20.8 billion by the research firm Gartner Inc. to a 30.7 billion estimate from data analyst IHS Markit Ltd.

If manufacturer behaviors don't change, more internet-of-things devices could mean more potential attack vectors that

14. U.S. House Energy and Commerce Committee, "Understanding the Role of Connected Devices in Recent Cyber Attacks," Nov. 16, 2016. https://energycommerce.house.gov/hearings-and-votes/hearings/understanding-role-connected-devices-recent-cyber-attacks

15. Ron Ross, Michael McEvilley and Janet Carrier Oren, "Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," *Systems Security Engineering*, NIST Special Publication 800-160: 1-219, November 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

16. Michael Mimoso, "Chinese Manufacturers Recalls IoT Gear Following Dyn DDoS," *Threat Post*, Oct. 24, 2016. https://threatpost.com/chinese-manufacturer-recalls-iot-gear-following-dyn-ddos/121496/

17. Bruce Schneier, "Regulation of the Internet of Things," *Schneier on Security*, Nov. 10, 2016. https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html

18. Israel M. Kirzner, *Competition and Entrepreneurship*, rev. ed., Liberty Fund, 2010.

19. Amy Nordrum, "Popular internet of things Forecast of 50 Billion Devices by 2020 is Outdated," *IEEE Spectrum: Technology, Engineering, and Science News,* Aug. 18, 2016. http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

20. U.S. Census Bureau, "U.S. and World Population Clock: Tell us what you think," accessed Feb. 9, 2017. https://www.census.gov/popclock/.

cyber criminals could exploit. According to research from Hewlett Packard Enterprise, 70 percent of the most common internet-of-things devices and infrastructure contain at least one security vulnerability.[21] Common vulnerabilities include lack of password security, insecure online user interfaces, inadequate encryption and overly broad user-access permissions. HPE's study found that 80 percent of internet-of-things systems did not require complex passwords and 70 percent did not encrypt data in transit.

The threat of proximate harm to owners of insecure internet-of-things devices is unknown. It is more likely that an individual will be the victim of a data breach. In 2015, cyber criminals accessed the records of 165 million Americans, roughly half the U.S. population.[22] In 2013, one in three victims of a data breach had their identity stolen. To date, the federal government's approach to address cyber risk has helped to move the conversation forward in three important ways: by facilitating development of voluntary cybersecurity standards, by helping address the lack of information about cyber incidents and by focusing on critical infrastructure.

FEDERAL APPROACH TO CYBERSECURITY POLICY

In 2013, then-President Barack Obama's Executive Order 13636 reignited a decadelong conversation on the role of government in cybersecurity.[23] The order instructed the National Institute of Standards and Technology to work with industry to develop voluntary cybersecurity standards to protect critical infrastructure, such as dams, electrical grids, financial institutions and transportation systems; asked the Department of Homeland Security to work with the private sector to develop an information-sharing program; and set goals for new hiring and training strategies for the cybersecurity workforce.[24] NIST's framework, originally released in February 2014 and updated most recently in January 2017, developed principles and best practices to help organizations manage, understand and communicate cyber risks. It highlighted five focus areas for cyber-planning, which it described as: identify, protect, detect, respond and recover.[25] It also included broad goals for technical outcomes, such as access control and data protection.

The framework is voluntary and compliance does not make companies immune from FTC enforcement actions. However, it appears from early surveys that companies that do not conform to the standards are more likely to be found liable after a cybersecurity incident.[26] Some industry associations have pushed back against further mandated technical standards for privacy or engineering, citing potentially duplicative or overly burdensome efforts.[27] Others have stressed the importance that the cybersecurity framework remain nonregulatory and voluntary, resisting any attempt by NIST to set compliance expectations for internet-of-things companies.[28]

Drawing on the NIST framework, DHS guidelines urge organizations to consider security during the system-engineering process, rather than the industry norm of adding firewalls, monitoring systems or applying encryption after the fact.[29] NIST also has published a guide for cybersecurity event recovery that stresses the importance of preparing cyber plans, policies and procedures.[30] These recommendations have implications for manufacturers of internet-of-things devices, as well as for networked infrastructure.

The Obama White House followed up Executive Order 13636 with Executive Order 13691 in 2015, which expanded the use of analysis organizations and information-sharing beyond critical infrastructure to any affinity groups that wanted to share threat information. In February 2016, Obama created the Commission on Enhancing National Cybersecurity, whose final report recommended public-private collaboration to address the internet of things as an area of special concern.[31] Action items included immediate collaboration between NIST and the internet-of-things industry to create voluntary standards organizations, as well as developing new cybersecurity standards, possible regulatory rulemaking to encourage adoption of those standards, a federal study

21. Hewlett-Packard Enterprise, "Report: internet of things Research Study," 2014. http://go.saas.hpe.com/fod/internet-of-Things

22. Identity Theft Resource Center, "Data Breach Reports," Dec. 29, 2015. http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

23. White House "Improving Critical Infrastructure Cybersecurity," Exec. Order No. 13636, 78 Fed. Reg. 11737, Feb. 12, 2013. https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

24. Eric A. Fischer, et al. "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress" Congressional Research Service, Dec. 15, 2014. https://www.fas.org/sgp/crs/misc/R42984.pdf

25. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", Version 1.0, Feb. 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214- final.pdf

26. Hanley Chew and Tyler G. Newby, "Privacy Alert: NIST Updates Cybersecurity Framework to Address Supply Chain Security," Fenwick and West LLP, Jan. 8, 2017. http://www.fenwick.com/Publications/Pages/Privacy-Alert-NIST-Updates-Cybersecurity-Framework-to-Address-Supply-Chain-Security.aspx.

27. Diane Honeycutt, "Views on Framework for Improving Critical Infrastructure Cybersecurity," Docket No. 151103999-5999-01], Feb. 23, 2016. http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_Symantec.pdf; http://www.itic.org/dotAsset/f/9/f9ef5f80-ffc5-4035-b274-87489605ab6e.pdf

28. CITA Wireless Association, "Views on the Framework for Improving Critical Infrastructure Cybersecurity," Feb. 23, 2016. http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_CTIA-The_Wireless_Association.pdf

29. U.S. Department of Homeland Security, "Strategic Principles for Securing the internet of things," Nov. 15, 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

30. Michael Bartock, et al., "Guide for Cybersecurity Event Recovery," Computer Security NIST Special Publication 800-184, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

31. Commission on Enhancing National Cybersecurity, "Report on Securing and Growing the Digital Economy," Dec. 1, 2016, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

on laws relating to internet-of-things device liability and increased research and development funding for cybersecurity.

There also have been legislative proposals intended to address the cyber-threat information gap. The Cybersecurity Information Sharing Act, signed by Obama in December 2015, seeks to improve the flow of communication between companies and federal agencies by offering legal immunity to companies that share information. While information-sharing can be a net positive for stakeholders in the cybersecurity community, there also are concerning aspects–namely the potential to expand government surveillance and to overshare personally identifiable information.[32]

Data-breach notification requirements reduce the information gap for a specific type of cyber event: the unauthorized access of certain types of user data. Two federal laws–the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act–require health and financial institutions to explain their information-sharing practices and to protect user data.[33] HIPAA requires health entities to provide notification following a breach of health information. In addition, 47 states, Puerto Rico and the District of Columbia legally require companies to notify customers of a breach of protected information—including health or personally identifiable information.[34]

More recently, the question of regulatory intervention in the internet of things has been the subject of a series of public workshops hosted by the Federal Trade Commission,[35] as well as a hearing of the Senate Commerce, Science and Transportation Committee.[36] In fact, the FTC recently filed a complaint against computer-networking manufacturer D-Link Corp., asserting it put U.S. consumers' privacy at risk by leaving its routers and webcams vulnerable to hackers.[37] The agency has brought similar cases against manufacturers ASUS and TRENDnet and it's likely the FTC will continue to bring charges against manufacturers for false claims of security.

A number of advocacy groups— including the Electronic Privacy Information Center and the Center for Democracy and Technology—have urged the FTC to implement strong privacy and security standards, citing extensive data collection in the home, a lack of privacy by design, the potential for harm to persons or their property, surveillance concerns and device access to sensitive information, such as health data.[38] These recommendations mirror the European approach to privacy regulation, which includes requiring consumer consent for data collection, mandating transparency, imposing accountability requirements for data practices, limiting data collection and making collected data available to the user.

Following a comment period and a workshop in 2016, the U.S. Commerce Department also has asserted a role in the burgeoning internet-of-things market, releasing a green paper that outlined their responsibility in an interagency approach to foster advancement of the internet of things.[39] The paper asserts the Commerce Department will be involved in standards adoption, promoting an open global environment for internet-of-things development, convening stakeholders to address policy challenges and providing policy input. Critically, it recognizes the risk of premature and excessive regulation and acknowledges the importance of allowing market entrants to experiment and mature.

The new administration also has highlighted cybersecurity as a priority. President Donald Trump has announced plans to create a "cyber review team" of individuals from law enforcement, the private sector and the military to assess cybersecurity risk.[40] Trump announced the selection of former New York City Mayor Rudy Giuliani as his cybersecurity adviser, a role focused on assembling meetings with companies facing cyber threats.[41] It is unclear how much impact on policy this role will allow him. While Giuliani has been working as chairman of Greenberg Traurig's global cybersecurity practice and is the CEO of the international security-consulting firm Giuliani Partners, many observers note it is unclear if he has sufficient technical knowledge or

32. Greg Nojeim, et al. "Letter to Senate Select Committee on Intelligence: Oppose CISA," June 26, 2014. http://www.rstreet.org/outreach/letter-to-senate-select-committee-on-intelligence-oppose-cisa/

33. Steptoe & Johnson LLP, "Comparison of US State and Federal Security Breach Notification Laws," Jan. 21, 2016. http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

34. National Conference of State Legislators, "Security Breach Notification Laws," Jan. 4, 2016. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

35. Federal Trade Commission, January 2015.

36. Senate Committee on Commerce, Science and Transportation, "The Connected World: Examining the Internet of Things," Feb. 11, 2015. http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=d3e33bde-30fd-4899-b30d-906b47e117ca&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=2&YearDisplay=2015.

37. Federal Trade Commission, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras," Jan. 5, 2017. https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

38. Center for Democratic Technology, "Re: Comments after November 2013 Workshop on the 'Internet of Things,'" Jan. 10, 2014, https://cdt.org/files/pdfs/iot-comments-cdt-2014.pdf.

39. Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

40. Donald J. Trump, "Donald J. Trump Promises Immediate Action on Cybersecurity in His Administration," *Remarks to the Retired American Warriors*, Oct. 3, 2016. https://www.donaldjtrump.com/policies/cyber-security

41. Michael Shear, "Rudy Giuliani's Cybersecurity Role Reflects Diminished Place in Trump World," *The New York Times*, Jan. 12, 2017, https://www.nytimes.com/2017/01/12/us/politics/rudy-giuliani-cyber-security-trump.html?_r=1.

experience to engage the issue effectively.[42] Encouragingly, in an interview on Fox News, he emphasized the importance of market forces: "My belief is, as always, that the answer to cybersecurity is going to be found in the private sector."[43]

The extent of the Trump administration's engagement on cybersecurity also remains to be seen. A continued emphasis on cybersecurity presents an opportunity to advance the discussion about the insecurity of internet-of-things devices.

GROWING CYBERSECURITY RISK IN THE INTERNET OF THINGS

Cybersecurity is often an afterthought for manufacturers of internet-of-things devices, either because they deem effective measures too costly to implement, because the risks are not understood or because options to mitigate risk are not available or affordable. As a result, many devices are not designed with secure features and cannot be updated or patched after they are sold. In October 2016, hackers using the Mirai malware hijacked a network of internet-of-things devices and used the resulting botnet to perform a distributed denial of service attack on Dyn Inc., a domain-name service provider. The attack disrupted access to such websites as Twitter, Netflix, Amazon and Spotify. It's thought that Mirai malware has infected more than a half-million devices, including more than 10,000 network cameras produced by the Chinese company Hangzhou Xiongmai Technology Co. Ltd.[44] As a result, the company recalled more than 4 million of their networked webcams, which relied on default passwords that many users never changed.

According to an industry survey, 73 percent of internet technology professionals believe security standards are not sufficient to protect the internet of things.[45] Because security is not often "baked in" during the design phase, or throughout the lifetime of a product, the internet of things faces heightened risk of cybercrime. In addition, the challenge posed by internet-of-things devices is unique, because the insecurity of one device affects the ecosystem as a whole. Where a property owner whose home is insecure would bear the full consequences of a robbery, the owner of an insecure device may unknowingly harbor malware that disrupts someone else's online experience. The device owner enjoys the concentrated benefit of using the device, but the costs of insecurity are dispersed throughout the network. The "infection" metaphor is apt. Malware infects connected devices and the resulting botnet is representative of an acute outbreak.

In 2016, service providers listed DDoS attacks as the largest security concern and most common threat.[46] DDoS attacks barrage a target website or application with a large volume of "junk" data or traffic. Such attacks are increasing in frequency and in magnitude, now topping 500 gigabits per second. For a point of comparison, the average internet connection speed in the United States is 12.6 megabits per second, where 1 gigabit is equal to 1,000 megabits.[47] DDoS attacks increasingly target cloud and domain-name services. Criminals also use them to demonstrate their attack capabilities, as part of extortion schemes or to distract from malware infiltration or data breaches.[48] U.S. companies are known to be particularly at risk, as they are targeted frequently and incur larger financial losses than global companies.[49] The top five industries that fell victim to cyber-attacks in 2015 were health care, manufacturing, financial services, government and transportation.[50]

Like malicious insider and web-based attacks, DDoS attacks are high cost. According to an industry survey by the software firm Arbor Networks, 86 percent of respondents estimated the cost of internet downtime to be up to $5,000 per minute.[51] A similar industry survey found that half of DDoS attacks last between six and 34 hours, with an estimated cost of $40,000 per hour.[52] This means that the average DDoS attack can cost about $500,000 for a firm.[53]

Those tallies do not include the ancillary costs of cyberattacks, which can lead to loss of intellectual property; loss of data (including consumer data or sensitive information); physical infrastructure damage; and business and supply-chain interruption. Researchers at RAND Corp. estimate the average data breach costs companies $200,000, although a majority of such events amounted to less than 0.4 percent of a company's annual revenues.[54] Data exfiltration attacks

42. Trevor Timm, "Rudy Giuliani is an absurd choice to defend the US from hackers," *The Guardian*, Jan. 13, 2017. https://www.theguardian.com/commentisfree/2017/jan/13/rudy-giulianis-not-fit-to-protect-the-us-from-hackers

43. Fox & Friends, "Rudy Giuliani to Head New Cyber Security Committee for Trump," Fox News Insider, Jan. 12, 2017. http://insider.foxnews.com/2017/01/12/rudy-giuliani-heads-cyber-security-committee-donald-trump

44. Mimoso, 2016.

45. Jeremy Seth Davis, "Three-quarters of industry pros say a breach caused by an IoT device is likely," SC Magazine, Oct. 23, 2015. https://www.scmagazine.com/three-quarters-of-industry-pros-say-a-breach-caused-by-an-iot-device-is-likely/article/533829/

46. Arbor Networks, 2016.

47. Akamai, "State of the Internet Report," 2016. https://content.akamai.com/pg7425-uk-soti-report.html

48. Arbor Networks, 2016.

49. PricewaterhouseCoopers, "Global Economic Crime Survey," 2016. http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

50. IBM X-Force Research, "IBM 2016 Cyber Security Intelligence," 2016. http://www-03.ibm.com/security/data-breach/cyber-security-index.html

51. Arbor Networks, 2016.

52. Incapsula, "Survey: What DDoS Attacks Really Cost Businesses," pp. 1-9, 2014. https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

53. Incapsula, p. 6, 2014.

54. Sasha Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cyber Security*, Aug. 8, 2016. http://cybersecurity.oxfordjournals.org/content/early/2016/08/08/cybsec.tyw001.

can be hard to detect. According to research firm Mandiant, the average lag time from initiation until a data breach is detected is 205 days.[55]

In some cases, data have national security implications or could affect relations with international allies. The 2015 hack of the U.S. Office of Personnel Management resulted in the loss of the sensitive personal information of 21.5 million federal employees, including the information of 19.7 million security-clearance applicants.[56] In 2009, a Chinese hacker acquired data relating to the F-22 and F-35 fighter jets from U.S. defense companies.[57]

The Online Trust Alliance indicated in a 2014 report that 90 percent of that year's breaches could have been prevented if organizations implemented basic cybersecurity best practices.[58] The Broadband Internet Technical Advisory Group has determined that the best current software practices for internet-of-things devices include shipping devices with current software; designing a mechanism for secure, automated software updates; employing strong authentication by default; using cryptography best practices; and testing and hardening internet-of-things device configurations.[59]

The Ponemon Institute estimates that one quarter of all breaches are due to human error,[60] including internal employee errors, as was the case with Hillary Clinton campaign chairman John Podesta's hacked email account. Podesta mistakenly clicked a link in a fraudulent phishing email that directed him to change his password, allowing hackers access to the account and 10 years' worth of his emails.[61] Such breaches can be prevented by encouraging basic security behavior, such as keeping devices up-to-date, increasing awareness about phishing and social-engineering attacks, using complex passwords with two-factor authentication and updating passwords regularly.

Combating an industrywide infection will require efforts to prevent, detect, mitigate and cure vulnerable devices. For device users and producers, security best practices must become habitual. For internet-of-things companies, proper cyber hygiene includes enforcing strong passwords and regular password changes; updating firewalls, anti-virus, anti-malware tools and other protection systems; encrypting sensitive data; implementing a data-loss protection solution that can monitor traffic; introducing vigorous updating and patching, including automatic patch deployment; and limiting configurations, ports, protocols and services to prevent remote access.[62] In the following sections, we will explore how industry, policymakers and third parties can offer incentives to adopt basic cybersecurity practices through market mechanisms.

CASE FOR A LIGHT-TOUCH REGULATORY APPROACH

As the internet of things continues to develop, policymakers should be careful not to construct overly restrictive regulatory regimes. Fear of insecure devices manufactured abroad or apprehensions about the privacy implications of data collection should not drive rash policy decisions. Rushing the rulemaking process could lead to poor implementation, exaggerated compliance costs and limited results.[63] Regulations may have unintended consequences that could strangle the internet-of-things industry while it's still in the cradle.

Heavily regulated industries experience fewer market entrants and slower employment growth, disproportionately affecting smaller firms and limiting competition.[64] Regulatory requirements can also dampen competition. In this way, regulations serve to shield large, well-represented companies from competition, because smaller companies can't afford to comply.[65] In effect, regulations act as a barrier to entry for entrepreneurs, allowing incumbent firms to raise prices, diminish quality and reduce expenditures on research and development.

55. Mandiant, "M-Trends 2015: A View from the Front Lines," FireEye, 2015. https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html

56. Jim Sciutto, "OPM government data breach impacted 21.5 million," *CNN Politics*, July 10, 2015. http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/

57. Justin Ling, "Man Who Sold F-35 Secrets to China Pleads Guilty," *Vice News*, March 24, 2016. https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty

58. Online Trust Alliance, "OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented," Jan. 21, 2015. https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

59. Broadband Internet Technical Advisory Group, "Internet of Things (IoT) Security and Privacy Recommendations: A Broadband Internet Technical Advisory Group Technical Working Group Report," November 2016. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

60. Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis," May 2015. https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

61. Joe Uchill, "Typo led to Podesta email hack: report," *The Hill*, Dec. 13, 2016. http://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack

62. Symantec Corp., "Internet Security Threat Report," Vol. 19, pp. 2-97, 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

63. Jerry Ellig, Patrick A. McLaughlin and John F. Morrall III, "Continuity, Change, and Priorities: The Quality and Use of Regulatory Analysis across U.S. Administrations," *Regulation & Governance*, 7:153–73, Aug. 13, 2012. http://onlinelibrary.wiley.com/doi/10.1111/j.1748-5991.2012.01149.x/abstract; see also Jerry Ellig and Rosemarie Fike, "Regulatory Process, Regulatory Reform, and the Quality of Regulatory Impact Analysis," Working Paper No. 13-13, Mercatus Center at George Mason University, July 2013. http://mercatus.org/publication/regulatory-process-regulatory-reform-and-quality-regulatory-impact-analysis

64. James Bailey and Diana Thomas, "Regulating Away Competition: The Effect of Regulation on Entrepreneurship and Employment," *Mercatus Center*, September 2015 https://www.mercatus.org/system/files/Bailey-Regulation-Entrepreneurship.pdf

65. Matthew Mitchell, "The Pathology of Privilege: The Economic Consequences of Government Favoritism," Mercatus Research, Mercatus Center at George Mason University, July 8, 2012. https://www.mercatus.org/publication/pathology-privilege-economic-consequences-government-favoritism

By one estimate, the accumulation of regulations in the United States between 1949 and 2005 slowed overall economic growth by an average of 2 percent per year, amounting to $277,100 per household.[66] Regulatory accumulation increases compliance costs, takes resources away from productive activities[67] and can negatively impact job and wage growth.[68] Moreover, excessive regulation can introduce uncertainty that pressures companies to move operations to jurisdictions with more favorable regulatory regimes.[69] Foreign competitors who do not face the same regulations may be able to undercut their regulated competitors, putting U.S. companies at a competitive disadvantage.

Regulation aimed at encouraging cybersecurity in the internet of things should emphasize performance standards over design standards. Performance standards specify the outcome of a policy and allow companies the flexibility to identify the best means or design to achieve it.[70] For example, a performance standard could state that data at rest on internet-of-things devices needs to be protected, whereas a design standard might specify the type of encryption or layer that needs to be encrypted. An unseen secondary consequence of design standards is that they remove the incentive for companies to find alternative solutions to achieve the same outcome. Given the broad number of functions served by networked devices, it is unlikely that a design standard will be effective for all use cases. Air gapping, data backups or data-masking techniques may work better for some internet-of-things applications. Furthermore, developments in encryption techniques, or in the sophistication of criminals, quickly may render a given design standard ineffective.

Furthermore, there can be problems with inconsistent or incorrect administration and enforcement of standards. Performance standards can also be restrictive or misdirected, but exhibit advantages over design standards because they are not as prescriptive.[71] Moreover, performance standards do a better job of aligning the incentives of companies and regulators, because they reward behaviors directed at the desired outcome rather than at compliance tasks.

Regulatory programs that rely on market-based incentives can have better, longer-lasting outcomes than regulations that focus on design standards. Industry can participate in self-regulation, as well, by recalling unsecure products, updating products or changing policies to address cybersecurity concerns. To the extent possible, policymakers should allow companies the flexibility to adapt to changing threats and address concerns as they arise.[72]

MARKET SOLUTIONS

Cyber insurance

Cyber insurance policies, which first appeared during the dot-com boom of the early 2000s,[73] allow businesses to transfer the liability and operational risks of cyber-attack or other internet-based risks to insurers. In its earliest forms, cyber insurance covered first-party property loss—damage to an insured's own infrastructure and equipment—as well as liability coverage to defend clients against lawsuits.

Today's cyber insurance can cover breach-response costs, such as attorneys' fees; breach notification to consumers; credit monitoring for consumers; call centers; public relations services; and technical forensic investigations to determine the origin of the attack and how it occurred. Other costs covered by cyber insurance include regulatory fines and responses to regulators, as well as legal defense and settlement costs. More recently, cyber-insurance solutions have included DDoS mitigation services and costs associated with internet downtime.[74] In one notable recent claim, the Los Angeles Community College District used their cyber-insurance policy to cover a $28,000 ransom after a ransomware attack paralyzed the college's computer network and email system.[75] Cyber insurance allowed the college to recover and learn from the attack.

Evidence shows the commercial cyber-insurance market is growing. As of June 2016, the National Association of Insurance Commissioners found that more than 500 insurers are

66. John W. Dawson and John J. Seater, "Federal Regulation and Aggregate Economic Growth," *Journal of Economic Growth*, pp. 1–41, January 2013. http://www4.ncsu.edu/~jjseater/regulationandgrowth.pdf

67. Testimony by Patrick A. McLaughlin, The Searching for and Cutting Regulations that are Unnecessarily Burdensome Act of 2014," House Committee on the Judiciary, Subcommittee on Regulatory Reform, Commercial, and Antitrust Law, Feb. 11, 2014 http://docs.house.gov/meetings/JU/JU05/20140211/101738/HHRG-113-JU05-Wstate-McLaughlinP-20140211.pdf

68. Keith Hall, "The Employment Costs of Regulation," Mercatus Center, March 2013. https://www.mercatus.org/system/files/Hall_EmploymentCosts_v3.pdf

69. W. Mark Crain and Nicole V. Crain, "The Cost of Federal Regulation to the U.S. Economy, Manufacturing and Small Business," *National Association of Manufacturers*, pp. 1-73, Sept. 10, 2014. http://www.nam.org/Data-and-Reports/Cost-of-Federal-Regulations/Federal-Regulation-Full-Study.pdf

70. David Hemenway, "Performance vs Design Standards," U.S. Department of Commerce, NIST, pp. 1-35, October 1980. http://gsi.nist.gov/global/docs/pubs/NIST-GCR_80-287.pdf

71. Id., pp. 2-3.

72. Consumer Technology Association, "Internet of Things: A Framework for the Next Administration," November, 2016. http://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf

73.Michael Menapace, "Written Testimony to Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security: Examining the Evolving Cyber Insurance Marketplace," March 19, 2015. https://www.commerce.senate.gov/public/_cache/files/90fa0bc7-8686-4b90-9a1b-3525cc62d4fe/8A982AD17B40EDD0101AD5974A36AD73.menapace-testimony-for-senate-hearing-on-cyber-insurance.pdf

74. Christine Marciano, "Cyber Insurance can serve as an Ideal DDoS Attack Response Plan," June 12, 2014, https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-can-serve-as-an-ideal-ddos-attack-response-plan/

75. Soloman Smith, "Update: Valleys Pays Ransom with Cyber Insurance," *The Valley Star*, Jan. 6, 2017, http://thevalleystar.com/valleys-pays-ransom-with-cyber-insurance/#sthash.bBt6GcLi.dpbs

supplying cyber insurance in the United States, with direct written premiums of nearly $484 million for standalone cybersecurity policies and nearly $1 billion for package policies.[76] Total written premiums are expected to double over the next four years from $4 to $8 billion in 2020.[77] However, it's worth noting that adoption varies significantly by industry. While the takeup rate in the retail, health and financial services sectors is around 80 percent,[78] less than 5 percent of the manufacturing sector has cyber-insurance coverage.[79]

Because insurers must be certain they take in sufficient premiums to cover the risks they take on, risk assessment is a crucial part of the insurance process, both in the underwriting (determining whether to insure a given risk) and ratemaking (determining what premium to charge for that risk) functions. The predictable effect of this risk-based pricing is to expand the market incentives for risk mitigation, just as insurers also have sought actively to improve building standards in risk-prone areas[80] and encouraged other kinds of loss-mitigation planning.[81]

Similarly, cyber insurance can help companies to reflect on possible risks and plan for them. Cyber insurance policies often offer monitoring services that decrease the time needed to respond to a threat.[82] During risk assessments, cyber insurers evaluate the applicant's security, sometimes with an on-site visit and almost always with an online questionnaire designed to measure security infrastructure, available budget, virus-protection programs, outsourcing, and testing and security procedures.[83] During on-site visits, the insurer may perform a technical assessment of a network's internal and external vulnerabilities, including a review of firewalls, routers and network configuration. In this way, insurers can hold businesses accountable to their cybersecurity plans by having policy provisions in place that prevent firms from making claims if they have not taken reasonable steps to maintain or improve their security.

Cyber-insurance policies often require insureds to make data-encryption and security-patch commitments. In addition to these benchmark security requirements to be eligible for a policy, actuarially sound premiums also provide incentives to insureds to adopt better cyber practices.[84] Improving authentication processes by, for example, removing default passwords would prevent password-stealing botnets from deputizing internet-of-things devices. Encryption of data at-rest and data in-transit can protect private information.[85] Firewalls, anti-virus software and anti-malware tools can also help to protect data. Developing, updating and patching practices help companies to address evolving cyber threats. During the design phase, manufacturers can limit configurations, ports and protocols to prevent remote access. Those insureds who demonstrate compliance with these kinds of good cyber-hygiene practices may enjoy discounts. Those who do not may not be able to obtain coverage at all.

Information is crucial for underwriters to assess risks. Toward that end, public and private information-sharing efforts encourage access to data on the frequency, extent and type of cyber-attacks. The 2014 NIST framework, developed to advance discussion of best cybersecurity practices, codifies common expectations of cyber risk as perceived by industry and government. The framework could offer a valuable underwriting and ratemaking tool for insurers, in that it represents a shared cyber-risk language for companies, third parties and policymakers that previously was absent.[86]

But cyber insurance is not a cure-all and the market has not yet developed to the extent that it can manage all potential risks. While estimates show that policies with $50 million limits would be able to cover roughly 92 percent of cyber-event claims,[87] some models estimate the likelihood of a major "black swan" event in the next decade that causes between $250 billion and $1 trillion in damage to critical information infrastructure to be between 10 and 20 percent.[88]

It can be hard to quantify exposure to cyber risks, especially when a loss by one company affects other parts of the network. The motives for cyber-attack are diverse, multiple

76. National Association of Insurance Commissioners, "Early NAIC Analysis Sheds Light on Cybersecurity Insurance Data," June 30, 2016. http://www.naic.org/Releases/2016_docs/cybersecurity_insurance_data_analysis.htm

77. Jonathan Camhi, "The Cyber Insurance Report: Market potential, top industries, and the major challenge to offering a fast-growing insurance product," *BI Intelligence*, Feb. 2, 2016.

78. Council of Insurance Agents and Brokers, "Cyber Insurance Market Watch Survey," October 2016. https://www.ciab.com/uploadedFiles/Resources/Cyber_Survey/102016CyberSurvey_Final.pdf

79. Ibid.

80. Mike Tsikoudakis, "Hurricane Andrew Prompted Better Building Code Requirements," *Business Insurance*, Sept. 19, 2012, https://www.businessinsurance.com/article/20120819/NEWS06/308199985

81. Zurich Insurance Co., "Report: Enhancing Community Flood Resilience: A Way Forward," May 2014. https://www.zurich.com/en/media/news-releases/2014/2014-0612-01

82. Id., p. 11.

83. Id., pp. 11-12.

84. Jay Kesan, Ruperto Majuca and William Yurcik, "Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study," University of Illinois at Urbana-Champaign, 2005. http://infosecon.net/workshop/pdf/42.pdf

85. Anurag Kumar Jain and Devendra Shanbhag, "Addressing Security and Privacy Risks in Mobile Applications," *Mobile and Wireless Technologies*, September/October 2012. https://pdfs.semanticscholar.org/aa53/1e41c4c646285b522cf6f33f82a9d68d5062.pdf

86. Federal Insurance Office, "Annual Report on the Insurance Industry," U.S. Department of the Treasury, pp. 1-81, September 2015. https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2015%20FIO%20Annual%20Report_Final.pdf

87. Martin Eling and Jan Hendrik Wirfs, "Cyber Risk: Too Big to Insure?," Institute of Insurance Economics, pp. 6-7, 2016. http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

88. Global Risk Network, "Global Risks 2010," World Economic Forum, January 2010 http://www.weforum.org/pdf/globalrisk/globalrisks2010.pdf

attacks can take place simultaneously or may repeat, business impact is hard to measure and attacks may take years to uncover and report. Risk assessments can be costly, with one small business reporting that getting insurance quotes and complying with the NIST framework took four months and cost more than $10,000.[89]

Given complaints by some in the business community about the cost of cyber coverage, especially for small and mid-sized firms, some policy analysts have begun to discuss the possibility of a temporary government backstop for cyber insurance,[90] similar to the $100 billion reinsurance backstop Congress created for terrorism risks in 2002. However, unlike terrorism risk in 2002, insurance and reinsurance markets are growing in their capacity and appetite for cyber risk. To the extent that some firms may have difficulty placing some kinds of cyber risks with third parties, there also are a variety of alternative risk-transfer mechanisms available, most notably company-owned captive insurers or closely held risk retention groups.

A closer examination of the problems with the Terrorism Risk Insurance Act, which has been renewed three times since its creation, should counsel policymakers to view any further "temporary" insurance backstops with skepticism.[91] Either a formal government backstop for cyber insurance or a system that hinges on future government bailouts would create moral hazard problems.[92] The government safety net not only reduces incentives to guard against risk, but such programs also displace private coverage options and prove politically difficult to unwind.

A robust private cyber insurance market will help raise the bar for device security, which is important for the entire internet ecosystem. Taking the steps necessary to ensure that such a market flourishes should be a policy imperative.

Filling the information gap

The lack of robust and broadly accessible experience data about past cyber events is a challenge for all parties involved in the cybersecurity and cyber-insurance markets. Key information associated with cyber incidents includes the type, severity, incident-detection methods used, incident response deployed, contributing causes, vulnerabilities, assets compromised, motive, timeline, risk-management approach, mitigation and prevention measures, impacts and costs.[93]

The Department of Homeland Security's Cyber Incident Data and Analysis Working Group has identified a number of obstacles to information sharing, including anonymization concerns, data security, cultural differences, perceptions of commercial disadvantage, internal process hurdles, technical design issues, problems with participation and misunderstandings about the value of information sharing.[94] CIDAWG proposed creating a Cyber Incident Data and Analysis Repository that would provide insurers and other stakeholders with information to develop coverage and risk-management solutions.[95]

While the insurance industry generally is supportive of CIDAWG's proposal, there are concerns about how the data repository would be implemented.[96] To secure participation, the repository would have to ensure contributors that submissions would be anonymous and secure. Inaccurate and inconsistent reporting would render the CIDAR less valuable, but more detailed reporting questions could risk prompting contributors to share details that reveal their identities. While the repository will not be government-operated, it is unclear how much access government will have. Also unclear is where the data should be housed, whether a university, a company, an insurer or some other third-party organization. Also, the incentives for larger insurers to participate, and share what would otherwise be proprietary underwriting data with smaller competitors, may prove to be weak.

If the data repository can overcome these obstacles, one would expect insurers will be able to expand coverage offerings to small and medium-sized businesses.[97] Insurers could reward better cybersecurity practices with lower insurance rates and encourage the adoption of best practices, such as the NIST framework. Moreover, policymakers, researchers and companies will have the information to inform public and private risk-mitigation strategies and to direct cybersecurity research and policy focus.

89. Ola Sage, "Prepared Testimony for Hearing on Examining the Evolving Cyber Insurance Marketplace," Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security, March 19, 2015. https://www.commerce.senate.gov/public/_cache/files/cfa8174a-e7f4-434a-9669-09282c0a8f1f/1572E3208FB577D440D5CF0DA13B9125.sage-testimony-for-the-record-march-2015-final.pdf

90. Judy Greenwald and Sarah Veysey, "Cyber Risk Insurance Backstop could Emerge in the Event of Catastrophic Attack," *Business Insurance*, Feb. 22, 2015. https://www.businessinsurance.com/article/20150222/NEWS06/303019998

91. Ibid.

92. Ian Adams, "The Promise and Limits of Private Cyber Insurance," R Street Institute, December 2016. https://www.rstreet.org/wp-content/uploads/2016/12/78.pdf

93. Department of Homeland Security, "Enhancing Resilience through Cyber Incident Data Sharing and Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository," September 2015. https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20FINAL_v3b.pdf

94. Ibid.

95. Ibid.

96. American Insurance Association, Email RE: National Protection and Programs Directorate's Cyber Incident Data Repository White Papers, May 24, 2016. https://www.dhs.gov/sites/default/files/publications/052416_AIA%20Letter_DHS_CIDAR_Final.pdf

97. Rep. Bennie G. Thompson, Letter RE: Docket No. DHS- 2015-0068, May 24, 2016 https://www.dhs.gov/sites/default/files/publications/052416_US%20HOR%20Letter_DHS_CIDAR_Final_0.pdf

Programs that share threat information with companies and the government are helping to fill in this information gap. Such programs include Facebook's ThreatExchange and the DHS's Cyber Information Sharing and Collaboration Program.[98] Threat-modeling can allow companies or federal agencies to identify and correct vulnerabilities in real time.[99]

On the other hand, consumers continue to face information deficiencies, as it is difficult for them to determine whether such products as routers, smart TVs, smart thermostats or webcams are secure. The public information gap about cyber events and vulnerabilities represents a market opportunity for entrepreneurs to create ratings bodies and voluntary certification organizations. By providing information about companies' cybersecurity track records, these entities could foster trust and exchange between consumers and internet-of-things device sellers.

Some of this is already happening. For example, Underwriters Laboratories introduced a cybersecurity assurance program to assess security risks in internet-of-things products.[100] The Online Trust Alliance recently published the second version of its "IoT Trust Framework" to serve as a risk-assessment guide for stakeholders.[101] The OTA guide details devices' design requirements and security processes, serving as a checklist for internet-of-things device-certification programs.

There's also a role for more informal processes to supply reputational information to consumers, as Yelp or Amazon reviews do today. The threat of a bad rating or review can prompt companies to adopt better cyber practices and hold companies accountable for data breaches or vulnerabilities. Businesses can gain a reputation for securing their products and consumers can know which products are safe.

CYBER INSURANCE FOR FEDERAL VENDORS

The federal government and its contractors are "the largest single producer, collector, consumer, and disseminator of information in the United States and perhaps the world."[102] As a consequence, federal agencies can use their power of the purse to signal to industry that considering security at all phases of the design process is paramount.

Given the risk and sensitivity of data held by the government–including IRS records, Social Security numbers, personnel records, public and private-sector intellectual property and classified information–cybersecurity must be a priority. The Office of Personnel Management data breach in 2015 led to the exposure of 21.5 million records, including Social Security numbers, and affected 6.7 percent of the U.S. population.[103]

Sensitive data also flows through contractor systems connected to government information-technology networks. In 2012, agencies reported that contractors performed one-third of all information-technology security duties.[104] As internet-of-things technologies develop, these devices will be present in a growing amount of IT systems, including those of the federal government.

Federal cybersecurity requirements for agencies began with the 2002 passage of the Federal Information Security Management Act. FISMA charged the White House Office of Management and Budget with agency oversight, required creation of a Federal Information Security Incident Center and delegated cybersecurity responsibilities to NIST.[105] The bill also appointed agencies to be responsible for the cybersecurity of their own information systems, as well as systems operated by contractors.[106]

The federal government also has taken steps to bolster cybersecurity protections by its contractors, using the acquisitions process. In 2013, the Department of Defense issued requirements for defense contractors to protect unclassified controlled technical information—defined as "technical information with military and space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure or dissemination"—from cyber intrusions and report incidents.[107]

98. Facebook for Developers, "ThreatExchange," 2016. https://developers.facebook.com/products/threat-exchange; see also Department of Homeland Security, "Cyber Information Sharing and Collaboration Program," May 4, 2016. https://www.dhs.gov/ciscp

99. Mark G. Hardy, "Beyond Continuous Monitoring: Threat Modeling for Real-time Response," *SANS Institute Infosec Reading Room*, Oct. 25, 2012. https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-threat-modeling-real-time-response-35185

100. Underwriters Laboratories, "UL Launches Cybersecurity Assurance Program," April 5, 2016. http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/

101. Online Trust Alliance, "IoT Trust Framework," Jan. 5, 2017. http://otalliance.actonsoftware.com/acton/attachment/6361/f-008d/1/-/-/-/-/IoT%20Trust%20Framework.pdf

102. White House Office of Management and Budget, "FY 2005 Report to Congress on Implementation of the E-Government Act of 2002," p. 5. March 1, 2005. https://georgewbush-whitehouse.archives.gov/omb/inforeg/reports/2005_e-gov_report.pdf

103. Jim Sciutto, "OPM Government Data Breach Impacted 21.5 Million," CNN Politics, July 10, 2015. http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/

104. U.S. Government Accountability Office, "Agencies Need to Improve Oversight of Contractor Controls," GAO-14-612, August 2014. http://www.gao.gov/assets/670/665246.pdf

105. Robert Nichols, et al., "Cybersecurity for Government Contractors," Briefing Papers Second Series No 15, April 2014. https://www.cov.com/-/media/files/corporate/publications/2014/04/cybersecurity_for_govt_contractors.pdf

106. 44 U.S.C.A. § 3544(a)(1)(A)(ii).

107. 78 Fed. Reg. 69,273 (Nov. 18, 2013) (adding DFARS subpt. 204.73 and the clause at DFARS 252.204-7012).

The Obama administration's Executive Order 13636 instructed the General Services Administration and DOD to make recommendations on the benefits and feasibility of incorporating cybersecurity standards in the federal acquisition process.[108] The resulting report contained suggestions that may be implemented over the next few years, including instituting baseline cybersecurity requirements as a condition for contracts, harmonizing and developing common definitions, creating a governmentwide risk-management strategy and requiring government to procure certain items from trusted sources.[109]

At least two of these recommendations could be fulfilled by requiring that federal internet-of-things contractors procure certain types of cyber-insurance coverage. In particular, such a requirement would provide incentives for contractors to adhere to baseline cybersecurity standards and demonstrate these companies as trusted sources. The addition of a cyber-insurance requirement in federal acquisitions also would be consistent with the efforts of government entities to improve cybersecurity among government contractors.

In 2014, Eli Dourado and Andrea Castillo of the Mercatus Center proposed having federal agencies themselves buy cyber insurance through a competitive bidding process.[110] While the doctrine of sovereign immunity exempts most federal agencies from direct claims of tort, the courts have found some longstanding exceptions.[111] In the case of a cyber-attack or data breach that stems from the insecurity of a contractor or vendor's system, the contracting agency also could have to expend resources on a host of ancillary costs, which can include DDoS mitigation services, forensic investigations, user notifications and data recovery. Rather than pass such costs onto the taxpayers, agencies and government purchasing agents should assert in contractual language their right to subrogate these liabilities from the contractor or vendor. Thus, contractors and vendors also should be asked to demonstrate they are capable of bearing financial responsibility for any cyber-liabilities they might create for the federal government, including the risk that a breach or attack will render the contractor or vendor unable to deliver or complete a project.

Given the incredibly broad range of activities engaged in and potential risks faced by different kinds of federal vendors and contractors—not to mention that firms of different types and sizes each will have their own insurance and risk-management needs—no one-size-fits-all requirement could possibly cover all cases. For some firms, financial responsibility could be demonstrated in ways other than insurance coverage, including through a surety or other performance bond, or by posting collateral or cash equivalents, such as a letter of credit. But for many, the most cost-effective means to make such demonstrations would be to procure insurance, whether it be a commercial general liability and/or directors and officers program that includes cyber coverage; a standalone cyber package; by ceding risks to a company-owned captive insurer; or by participation in a risk retention group focused on cyber liabilities.

In contrast to enforcing specific security standards, stipulating a financial responsibility requirement would ensure that federal contractors evolve their security practices to find the most cost-effective risk-management strategies available. Aligning company incentives with market incentives will lead to better outcomes for the internet of things and for information security.

The implementation of a financial responsibility requirement for internet-of-things vendors would fall under the jurisdiction of the General Services Administration, which runs the Federal Acquisition Service responsible for awarding contracts to vendors. The requirement will have to be balanced to ensure that taxpayers are not held accountable for the poor cyber-hygiene or risk-management practices of federal contractors, but not to be so risk-averse as to add unnecessary costs to vendors or the government. For example, it may be prudent to cap the requirement to demonstrate financial responsibility to the size of a given contract. While it is possible for a contractor to create liabilities for the federal government far in excess of the value of their contract, uncapped liability could be unduly burdensome on smaller contractors

A vendor requirement intended to help with internet-of-things adoption could be implemented through an executive order, through a law enacted by Congress or through a guidance requirement issued by OMB or GSA. At the very least, requiring that federal internet-of-things vendors demonstrate a cyber plan to mitigate risk from DDoS attacks or data breaches will prompt federal contractors to examine their vulnerabilities more closely.

CONCLUSION

The internet of things introduces new attack vectors and has facilitated an increase in distributed denial of service attacks, among other types of cyberattacks. In the context of DDoS attacks, the lack of cybersecurity is often viewed as a demonstration of market failure. It should instead be

108. E.O. 13636 § 8(e).

109. General Services Administration and Department of Defense, "Improving Cybersecurity and Resilience through Acquisition," Jan. 23, 2014. http://www.defense.gov/news/Improving-Cybersecurity-and-ResilienceThrough-Acquisition.pdf

110. Eli Dourado and Andrea Castillo, "Why the Cybersecurity Framework Will Make Us Less Secure," Mercatus Center, April 17, 2014. https://www.mercatus.org/publication/why-cybersecurity-framework-will-make-us-less-secure

111. John Lobato and Jeffrey Theodore, "Briefing Paper No. 21: Federal Sovereign Immunity," Harvard Law School Federal Budget Policy Seminar, May 14, 2006. http://www.law.harvard.edu/faculty/hjackson/FedSovereign_21.pdf

viewed as a market opportunity for private actors to lower the cost of information exchange or to help companies mitigate cybersecurity risks. Policymakers can play a role in supporting market-based solutions like cybersecurity-assurance programs, information-sharing programs and adoption of cyber insurance.

One positive step policymakers can take to encourage adoption of good cyber practices is to leverage the power of the purse[112] to select government-facing internet-of-things vendors that have demonstrated their commitment to cybersecurity by employing appropriate risk transfer tools like cyber insurance. Encouraging the adoption of cyber insurance will help to usher in a culture of preparedness by offering incentives to companies that improve their basic security posture. It will also help companies to understand cyber risk and internalize the cost of device insecurity.

Policymakers should avoid any regulatory approaches that would require design standards rather than performance standards. Design standards include rules that would require products to use certain protocols or communication standards deemed secure, whereas performance standards would set a desired safety outcome without specifying the means to achieving it. This would motivate companies to focus on compliance, rather than security. Legislating specific technical solutions would codify easily outdated features, limit U.S. competitiveness abroad and stunt experimentation.

Market approaches to internet-of-things insecurity include adoption of cyber insurance, technical and managerial solutions, industry-led initiatives and voluntary certification and ratings efforts. In pursuing these efforts, industry leaders, third parties and policymakers can establish an environment where the security of connected devices is the norm rather than the exception.

ABOUT THE AUTHOR

Anne Hobson is a technology policy fellow with the R Street Institute, specializing in free-market approaches to emerging technologies, including virtual reality, artificial intelligence, the internet of things and the sharing economy.

Anne joined R Street in September 2016, having most recently served as a policy associate at Facebook's Washington office. She is an alumna of the Mercatus Center MA Fellowship at George Mason University, where she worked with the technology policy program, and was new media manager with The American Spectator as part of the Koch Associate Program.

112. Kate Stith, "Congress' Power of the Purse," *The Yale Law Journal* 97, no. 7 (June 1988): 1343–96.