Security Shield:
A Label to Support Sustainable Cybersecurity

Public Knowledge

Megan Stifel
Dylan Gilbert
Mark Peterson

Acknowledgements

The authors wish to thank the individuals and organizations that attended a 2018 Cyber/Week roundtable on this paper. Additionally, we’d like to thank Beau Woods, the Internet Society, and others for their feedback. This paper, along with other Public Knowledge cybersecurity works, was made possible by the generous support of the Hewlett Foundation.

Introduction

Public Knowledge recently proposed that stakeholders improve cybersecurity and foster innovation by drawing upon time-tested principles from sustainability management.[1] Transitioning to a sustainable approach to cybersecurity embraces the principles of shared responsibility and collective action, frames business costs associated with improved security as an investment in the internet ecosystem, encourages broad adoption of risk-management practices, and supports consumer engagement. The proposal made a series of operational and policy recommendations for actors across the internet ecosystem. It also asked for feedback on which actions were best to focus on first, what policy challenges stand in the way, and what incentives could spur broader adoption of these actions. After collecting feedback and reviewing some of those recommendations, the next phase will take a deeper look at the actions considered most impactful or with the longest development time.

One of the key points in discussions about the white paper has been the government's role in improving incentives for stakeholders to implement sustainable cybersecurity practices. This includes the need to raise social awareness, such as through education and labeling schemes, which can guide consumer choices, and possibly to introduce more coercive incentives, such as reevaluating frameworks for liability. In general, labeling consumer products encourages the consumer toward the preferred choice.[2] A cybersecurity labeling scheme is a viable mechanism for furthering sustainable cybersecurity practices in the context of consumer-facing Internet of Things (IoT) products. This paper proposes the creation of a "Security Shield" label to spur the market, to build consumer trust, and to foster a sustainable approach to cybersecurity in the IoT ecosystem and beyond.

The government's ability to stimulate the marketplace has been effectively demonstrated in environmental conservation and sustainability. Programs like Energy Star have provided non-regulatory incentives to industry to drive innovation, and statutory and common law legal claims have pressured companies to internalize negative externalities their activities may have on the ecosystem.[3] Applying these successful programs to cybersecurity could have significant positive impact in both the U.S. and internationally. Providing consumer-facing labels, indicating which products are assessed to be more secure than others according to consensus-developed capabilities baselines and standards, enables companies to compete on security in order to

[1] *See* Megan Stifel, *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*, Public Knowledge (Apr. 2018), https://www.publicknowledge.org/documents/securing-the-modern-economy-transforming-cybersecurity-through-sustainabili.

[2] *See*, *e.g.*, John M. Blythe and Shane D. Johnson, *Rapid evidence assessment on labeling schemes and implications for consumer IoT security*, 5 (Dawes Centre for Future Crime at UCL, 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf.

[3] *See, e.g.*, Clean Air Act § 304, 42 U.S.C. § 7604 (2012) (establishing a private right of action for certain violations of the statute); Clean Water Act § 505, 33 U.S.C. § 1365 (2012) (protecting a common law right of action for damages due to violation of the statute or to seek enforcement of the statute).

differentiate their products, and empowers consumers to have an informed influence on the market. In the same way that programs like Energy Star provided a means for manufacturers to incorporate and improve energy efficient designs, a labeling program for cybersecurity can encourage a secure-to-market approach for new devices and associated software. This will be particularly important as the Internet of Things dramatically expands the number of internet-enabled devices over the next decade.

The Emergence of a Cybersecurity Labeling Scheme

The 2016 Commission on Enhancing National Cybersecurity Report on Securing and Growing the Digital Economy recommended some form of labeling scheme to educate consumers on the relative security of devices and programs. The report stopped short of recommending a course of action, but distinguished between two potential options: a simple Energy Star-like mark, or a more detailed materials list-style label.[4] In 2017 the National Telecommunications and Information Administration Multistakeholder Process on Internet of Things Security Upgradability and Patching identified updatability as a capability that should be communicated to consumers, and identified a label as one method to do so.[5] More recently, the May 2018 Report to the President "Enhancing Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," ("Botnet Report") identified an IoT Line of Effort, Raising the Bar for IoT Security, and included as its first workstream the development of robust markets for trustworthy IoT devices.[6] It identified several tasks toward this end, including the development of a core security capability baseline, development of a consumer IoT security baseline, establishment of assessment programs for consumer IoT devices, and exploration of voluntary labeling approach for consumer IoT. The Botnet Report also called for the development of Guidelines for Software Component Transparency, the substance of which is similar to the materials list-style label. While both options have their uses, at this stage in the market's development a program similar to Energy Star is likely the more useful of the two for establishing baseline standards, addressing information asymmetries that undermine consumer trust, and driving innovation in cybersecurity.

Energy Star's strategic vision provides some useful principles for a cybersecurity labeling program. The program should seek to provide a common, objective basis for what constitutes a

[4] *See* Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy,* 30 (Dec. 1, 2016), https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[5] Multistakeholder Process on Internet of Things Security Upgradability and Patching, *Communicating IoT Device Security Update Capability to Improve Transparency for Consumers*, at 1 (July 18, 2017), https://www.ntia.doc.gov/files/ntia/publications/communicating_iot_security_update_capability_for_consumers_-_jul_2017.pdf; *see also* Federal Trade Commission Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers," https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

[6] *See* Report to the President "Enhancing Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats ("Botnet Report"), 43-44 (May 30, 2018), https://www.commerce.gov/sites/default/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

highly secure system, device, or program, it should provide an easy way to identify qualified products, and it should be coupled with education and outreach programs to build and sustain demand for qualifying products.[7] The other key to the Energy Star program has been identifying products that are cost-effective for purchasers, at least functionally equivalent to non-qualifying products, and broadly available. This constraint is critical to pushing the baseline standard forward and ensuring a continuing demand for qualifying products. State and federal support for the Energy Star program through tax cuts, rebates, subsidies, and direct purchases of qualifying products has also been important in sustaining the program and driving towards the overall public goal—a more sustainable, resilient energy market.

Today, the emergence of a cybersecurity labeling program seems almost inevitable. Equipment manufacturers are already developing their own internal standards, consumer advocacy groups are outlining requirements, and some governments are moving to regulate directly. The success of the Energy Star program argues for another alternative: voluntary participation in a program that develops consensus security baseline capabilities and standards, based on sustainable cybersecurity principles, assessed independently and identified by a government-recognized label.

A Brief History of Energy Star

Energy Star is a nonregulatory, opt-in, program administered by the Environmental Protection Agency ("EPA") and the Department of Energy that awards a consumer-facing label to qualifying products, identifying those that are the most energy-efficient in a given category, e.g., home appliances and electronics. Energy Star certification can also extend to commercial buildings and homes. It is generally regarded as one of the most successful and recognizable government-administered programs of the last quarter-century – more than 90% of U.S. households recognize and understand the label.[8] The EPA estimates the program has saved consumers over $430 billion in energy costs since its inception – in addition to saving more than 4.6 trillion kWh of electricity and preventing 2.8 billion metric tons worth of greenhouse gas emissions.[9] It is a rare example of successful market-guiding program with support from consumer advocates, corporations, and both political parties.[10]

[7] *See Energy Star Products Program Strategic Vision and Guiding Principles*, EPA, https://www.energystar.gov/ia/partners/prod_development/downloads/ENERGY_STAR_Strategic_Vision_and_Guiding_Principles.pdf?da2b-e159 (last visited July 5, 2018).

[8] *See* Energy Star, *Energy Star by the Numbers – 2016*, EPA, https://www.energystar.gov/sites/default/files/asset/document/Archive%20-%202016%20By%20the%20Numbers.pdf.

[9] *Id.*

[10] *See, e.g.,* Taryn Holowka, *Energy Efficiency: A Rare Bipartisan Consensus*, Real Clear Politics (Apr. 10, 2018), https://www.realclearpolitics.com/articles/2018/04/10/energy_efficiency_a_rare_bipartisan_consensus_136752.html; Mary H.K. Farrell, *Proposed Federal Budget Eliminates Energy Star*, Consumer Reports (May 23, 2017), https://www.consumerreports.org/appliances/proposed-federal-budget-eliminates-energy-star/; Letter from Industry in Support of Energy Star, Alliance to Save Energy (Apr. 24, 2017), https://www.ase.org/sites/ase.org/files/industry_support_letter_for_energy_star-final_5.0.pdf.

The modern Energy Star program began in the early 90's as "Energy Star Computers," a surprisingly narrow program drawing from the same principles as the EPA's Green Lights program.[11] Green Lights tackled one aspect of the energy efficiency problem, commercial lighting, by encouraging companies to upgrade their lighting systems.[12] As an incentive to invest in more efficient lighting, the EPA agreed to provide information on available technology and financing options, as well as public recognition for companies meeting their goals. The Green Lights approach recognized that there were economic benefits to adopting efficient technology that the EPA could market to private actors, and that real gains could be made by taking incremental, narrowly targeted steps. This approach informed Energy Star Computers, which encouraged computer manufacturers to reduce their products' overall energy consumption by implementing a sleep feature, entering a low-power state when idle for a long period.[13]

The EPA originally derived its authority for the Energy Star program through the Clean Air Act's mandate that the agency should "develop, evaluate, and demonstrate non-regulatory strategies and technologies for air pollution prevention," with opportunities for participation by industry and public stakeholders.[14] The original Energy Star Computers program rapidly expanded to include other pieces of office equipment, appliances, commercial buildings, and homes. In 2005 Congress moved to codify Energy Star in order to expand its scope and improve consumer education on energy efficiency.[15] The Energy Policy Act ("EPAct") of 2005 mandates that the Department of Energy and EPA maintain, "a voluntary program to identify and promote energy-efficient products and buildings in order to reduce energy consumption, improve energy security, and reduce pollution through [labeling and communication] about products and buildings that meet the highest energy conservation standards."[16] The EPAct also gives statutory weight to earlier Executive Orders requiring federal agencies to purchase Energy Star qualifying products

[11] *See generally The Climate is Right for Action: Voluntary Programs to Reduce Greenhouse Gas Emissions*, EPA (Oct. 1992).

[12] *See Introducing…The Green Lights Program*, EPA (Dec. 1993), https://nepis.epa.gov/Exe/ZyNET.exe/2000C67F.txt?ZyActionD=ZyDocument&Client=EPA&Index=1991%20Thru%201994&Docs=&Query=&Time=&EndTime=&SearchMethod=1&TocRestrict=n&Toc=&TocEntry=&QField=&QFieldYear=&QFieldMonth=&QFieldDay=&UseQField=&IntQFieldOp=0&ExtQFieldOp=0&XmlQuery=&File=D%3A%5CZYFILES%5CINDEX%20DATA%5C91THRU94%5CTXT%5C00000008%5C2000C67F.txt&User=ANONYMOUS&Password=anonymous&SortMethod=h%7C-&MaximumDocuments=1&FuzzyDegree=0&ImageQuality=r75g8/r75g8/x150y150g16/i425&Display=hpfr&DefSeekPage=x&SearchBack=ZyActionL&Back=ZyActionS&BackDesc=Results%20page&MaximumPages=1&ZyEntry=2.

[13] *See Energy Star Computers*, EPA, 1 (Sep. 11, 1992), https://nepis.epa.gov/Exe/ZyNET.exe/2000T10J.txt?ZyActionD=ZyDocument&Client=EPA&Index=1991%20Thru%201994%7CHardcopy%20Publications&Docs=&Query=Energy%20Star%20&Time=&EndTime=&SearchMethod=2&TocRestrict=n&Toc=&TocEntry=&QField=&QFieldYear=&QFieldMonth=&QFieldDay=&UseQField=&IntQFieldOp=0&ExtQFieldOp=0&XmlQuery=&File=D%3A%5CZYFILES%5CINDEX%20DATA%5C91THRU94%5CTXT%5C00000016%5C2000T10J.txt&User=ANONYMOUS&Password=anonymous&SortMethod=-%7Ch&MaximumDocuments=15&FuzzyDegree=0&ImageQuality=r85g16/r85g16/x150y150g16/i500&Display=hpfr&DefSeekPage=x&SearchBack=ZyActionE&Back=ZyActionS&BackDesc=Results%20page&MaximumPages=1&ZyEntry=1&SeekPage=x.

[14] 42 U.S.C. § 7403(g).

[15] *See* 151 Cong. Rec. H2193 (daily ed. Apr. 20, 2005) (statement of Rep. Barton) ("The bill . . . expands the Energy Star program to tell American consumers what products save the most energy.").

[16] 42 U.S.C. § 6294a(a).

where possible.[17] Today, "Energy Star Products" covers more than 60 categories of home and commercial devices.[18]

Congress allocates appropriations for the Energy Star Program under the EPA's Atmospheric Protection Program, with a requested $46 million to administer the program for fiscal year 2019.[19] Recent proposals to either eliminate the program[20] or shift to a user-fee collection model[21] have encountered resistance from members of Congress, industry groups, and consumer advocates.[22]

Existing Cybersecurity Assessment and Labeling Efforts

Thus far, cybersecurity assessment programs are evolving along three tracks: industry trade associations are developing standards for their own members; civil society and consumer advocacy groups are establishing frameworks for the public at large; and national and international standards associations are publishing independent criteria.

Several domestic efforts are underway that could support labeling schemes for consumer IoT devices. In August 2018, CTIA, a wireless industry trade association, unveiled a cybersecurity certification program for LTE and Wi-Fi enabled IoT devices.[23] Wireless operators, technology companies, security experts, and testing laboratories collaborated to create the program's plans and testing requirements to build upon the National Telecommunications and Information Administration ("NTIA") and National Institute of Standards and Technology ("NIST") IoT security recommendations.[24] While association-driven labeling programs can be helpful for pushing the ecosystem towards broad adoption, because such testing guides often prioritize speedy

[17] *See* 42 U.S.C. § 8259b; *see also* Exec. Order No. 12845, Requiring Agencies To Purchase Energy Efficient Computer Equipment, 58 Fed. Reg. 21,887 (Apr. 21, 1993); Exec. Order No. 13123, Greening the Government Through Efficient Energy Management, 64 Fed. Reg. 30,851 (June 8, 1999).

[18] *See Energy Efficient Products*, EPA, https://www.energystar.gov/products (last visited Jul. 10, 2018)

[19] *See* United States Environmental Protection Agency Fiscal Year 2019 Justification of Appropriation Estimates for the Committee on Appropriations, EPA at 153-54 (Feb. 2018), https://www.epa.gov/sites/production/files/2018-02/documents/fy-2019-congressional-justification-all-tabs.pdf.

[20] *See FY 2018 Budget in Brief*, EPA, 65 (May 2017), https://www.epa.gov/sites/production/files/2017-05/documents/fy-2018-budget-in-brief.pdf.

[21] *See FY 2019 Budget in Brief*, EPA, 18 (Feb. 2018), https://www.epa.gov/sites/production/files/2018-02/documents/fy-2019-epa-bib.pdf.

[22] *See, e.g.*, Timothy Cama, *Trump's plan for Energy Star sparks industry uproar*, The Hill (Feb. 22, 2018), https://thehill.com/policy/energy-environment/374940-trumps-plan-for-energy-star-sparks-industry-uproar; Marc Gunther, *Killing Energy Star: A Popular Program Lands on the Trump Hit List*, Yale Environment, 360 (May 4, 2017), https://e360.yale.edu/features/killing-energy-star-a-popular-program-lands-on-the-trump-hit-list.

[23] *See generally CTIA Cybersecurity Test Plan for IoT Devices*, CTIA, 5 (Aug. 2018), https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0.pdf ("For the purpose of this document, an IoT device contains an IoT application layer that provides identity and authentication functionality and at least one communications module supporting either LTE or WiFi®.").

[24] *See Wireless Industry Announces New Cybersecurity Certification Program for Cellular-Connected IoT Devices*, CTIA (Aug. 21, 2018), https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program.

certification and ease of market access over adoption and consumer education, they may not be the most effective approach to build consumer trust.

Civil society organizations have also undertaken various baseline development and labeling-related efforts. Mozilla,[25] in partnership with TrustCon, has launched a Trustable Technology Mark to help consumers assess the privacy and security of their home IoT devices.[26] The devices may be evaluated by representatives from TrustCon against five criteria: privacy & data practices, transparency, security, stability, and openness.[27] Alternatively, manufacturers can self-certify, but they must publish their assessment with an open license.[28] Although not a labeling program, The Internet Society, through its Online Trust Alliance ("OTA") initiative, has launched an IoT Trust Framework, which seeks to differentiate itself from other similar frameworks by focusing on the full privacy and security lifecycle and incorporating the entire IoT ecosystem, not just devices.[29] Civil society and private companies have also joined forces to introduce the Digital Standard, "an ambitious, open, and collaborative effort to create a digital privacy and security standard."[30] One goal of the Digital Standard is to equip consumers to be well-informed about the products that they buy.[31] The Standard does not, however, feature a consumer-facing labeling scheme, opting instead to focus on using the standard to allow testing organizations to evaluate and report to consumers on whether products are protecting consumer security and privacy.[32]

Internationally, the European Commission has set forth a legislative proposal to strengthen the European Union Agency for Network Security Information (ENISA), which is awaiting final review before passage.[33] In addition to reinforcement of the EU cybersecurity agency's mandate, the EU Cybersecurity Act[34] (ECA) would establish an ICT cybersecurity certification framework.[35] The ECA certification framework, "would provide for EU-wide certification schemes with a comprehensive set of rules, technical requirements, standards and procedures" that ENISA would prepare in cooperation with a European cybersecurity certification

[25] While somewhat of a hybrid entity, because Mozilla is a non-profit we include them with other members of civil society for purposes of this section.

[26] *See* Matthew Hewes, *Mozilla and ThingsCon launch certification mark for secure IoT devices*, The Next Web (last visited Jan. 24, 2019), https://thenextweb.com/security/2018/12/06/mozilla-and-thingscon-launch-certification-mark-for-secure-iot-devices/.

[27] *Id.*

[28] *See* Trustable Technology Mark Application Form, https://trustabletech.org/apply/.

[29] *See* Internet Society, *IoT Trust by Design*, https://www.internetsociety.org/resources/doc/2018/iot-trust-by-design.

[30] *Digital Standard*, Digital Standard, https://www.thedigitalstandard.org/ (last visited Sep. 26, 2018).

[31] *See id.*

[32] *See Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace*, Consumer Reports (Mar. 06, 2017), https://www.consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_consumers_security_and_privacy_in_complex_marketplace/.

[33] *See generally* Mar Negreiro, *ENISA and a new cybersecurity act,* europarl.europa.eu (Sept. 6, 2018), http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.

[34] EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act), 2017/0225 (COD), https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en.

[35] *See* Negreiro, *supra* note 34 at 6.

group (ECCG).[36] After adoption of the certification scheme, a product manufacturer or ICT service provider could apply for certification with a conformity assessment body of its choice, with accreditation issued for a maximum of five years.[37]

The United Kingdom has introduced a Code of Practice for Consumer IoT Security based on "thirteen outcome-focused guidelines," which targets manufacturers but also provides guidance for consumers of IoT smart devices.[38] In 2018 Canada launched a multistakeholder process: Enhancing IoT Security, which includes a working group on labeling.[39] Together, the EU, Canadian, and UK-driven efforts are helping to push international developments in the right direction. However, while a pre-market evaluation can enhance the security of products going to market, market surveillance, including patchability, lifecycle management, and ongoing assessments, are also critical to enhancing security over the longer term, particularly given the rapidly evolving IoT market. The Canadian process incorporates these elements and could serve as a model for U.S. and broader markets.

These security capabilities baselines are an important development and signal maturation within the marketplace. Still, there will be some products that make it to market yet fail to follow best practices. To reduce the risk such insecure products pose to the internet ecosystem and trust in it, consumers need to be able to distinguish among more and less secure products. In light of the number and variation among baselines and the absence of a domestically recognized label to inform the market of conformance with a baseline, an opportunity exists for the U.S. government to convene a process to advance a globally interoperable baseline development and labeling process.

Practical Considerations in Developing a Consumer Cybersecurity Label

In considering the utility and viability of a consumer IoT cybersecurity labeling program, four key questions assist in focusing the discussion:

- Attestation: An effective security label will attest to a consensus security baseline or best practices. What criteria should be included in such a baseline?
- Assessment: Who or what should oversee the assessment process to verify the attestation?
- Attributes: What types of information should the label contain and how should the information be conveyed, e.g., what should the label look like?
- Implementation: How should the program be implemented?

[36] *Id.* at 8.

[37] *Id.*

[38] *See* U.K. Department for Digital, Culture Media & Sport, *Code of Practice for Consumer IoT Security* (Oct. 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf.

[39] *See, e.g.*, Canadian Multistakeholder Process: Enhancing IoT Security, *Report on Fourth Multistakeholder Meeting*, https://iotsecurity2018.ca/wp-content/uploads/2018/12/IoT-Security-Report-Meeting-4-November-20.pdf.

Attestation

Rather than focus initially on quantifiable security metrics—which arguably do not exist yet in a manageable form—a cybersecurity labeling program should instead start with a focus on qualifiable best practices in design and manufacturing. There are essentially three ways to identify these practices: industry-led development, national standards body development (through agencies like NIST), or through national contribution to an international standards body (e.g., the International Organization for Standardization ("ISO"). While it may be reasonable to develop unique national standards, it is wiser to develop standards with international application in mind.

The need for quantifiable metrics is one of the key challenges to implementing a rating scheme like Energy Star's in the cybersecurity context. A mature rating scheme necessarily requires discrete, objective measures of performance to analyze in order to generate metrics.[40] The conventional wisdom in cybersecurity has long been that threat vectors change too rapidly for most metrics to be meaningful, and that the variety of both threats and targets renders a "one size fits all" approach ineffective and inappropriate.[41] In addition, many commonly proposed measures, such as port scan rates and patch update completion, are either not clearly defined or not uniformly applied, limiting their accuracy and, therefore, their usefulness.[42]

For this reason, it is likely more useful to examine business practices at the design and manufacturing stages as well as post market, e.g., estimated product lifecycle and patching, as a way to gauge product security. Companies can attest to certain practices - for example early engagement with security researchers, improving supply-chain rigor, or taking efforts to reduce code complexity - in exchange for recognition.[43] In the absence of quantifiable metrics, these attestations give manufacturers a way to communicate their efforts and corporate values to consumers. In the same way that Energy Star gave manufacturers a way to display their products' energy conserving attributes, a Security Shield label allows them to show that cybersecurity is "an integral part of [their] development process."[44] Further, objective and observable attestestations can be independently, publicly verified (for marketed products) and tie into well-understood legal and government enforcement capabilities.

[40] A note on terminology: broadly, "measurement" refers to the collection of data on discrete factors, and a "metric" is derived by comparing two or more measurements to a predetermined baseline. For more, *see* Wayne Jensen, *NISTIR 7564: Directions in Security Metrics Research*, National Institute of Standards and Technology, 3-4 (Apr. 2009), https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf (last visited Sep. 26, 2018).

[41] *See generally,* Larry Clinton, *Metrics? What Metrics? Finding the Missing Link to the NIST Cybersecurity Framework*, Internet Security Alliance (May 31, 2017), https://isalliance.org/metrics-what-metrics-finding-the-missing-link-to-the-nist-cybersecurity-framework/ (last visited Sep. 26, 2018).

[42] *See* Paul E. Black, et al., *Cyber Security Metrics and Measures*, National Institute of Standards and Technology at 3, https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51292 (last visited Sep. 26, 2018).

[43] For an illustrative example, *see* I Am The Cavalry, *Five Star Automotive Cyber Safety Framework* (Feb. 2015), https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf.

[44] Rio Declaration on Environment and Development at 2 (1992), http://www.unesco.org/education/pdf/RIO_E.PDF (discussing environmental protection's importance to sustainable development).

Focusing on design and manufacturing practices also helps address one of the major weaknesses of a single pre-market assessment for cybersecurity. In contrast to Energy Star, Security Shield examines highly dynamic products. It is axiomatic that no software is bug-free, and any company seeking a reasonable time-to-market is likely to release flawed products—and those flaws may, in good faith, not be known at the time of release. With software, however, patching can remedy many—if not most—issues. It can also create new ones. At the same time, malicious actors are able to apply far more pressure on products "in the wild" than reasonable in-lab tests, and eventually discover ways to exploit hidden bugs. Together, these factors suggest that relying on a snapshot product test to award a Security Shield label would render the label largely irrelevant, because the practical security "quality" of any single product is likely to vary over time.

Private certifying organizations may push complementary standards in order to capture sections of the market not covered by this program. Including multiple stakeholders in development and allowing third-party certifiers to take part in the process may mitigate the chance that competing standards will arise. The risk of eventual confusion must be weighed against the benefit of more—or less—robust private standards. Ultimately, baseline standards should be developed with a goal of global interoperability. Keeping the international market in mind during development could help forbear more strident or conflicting global alternatives and lead the development of international standards.

Any policy effort to improve cybersecurity will require broad commitment from a variety of stakeholders in order to have a meaningful impact. Often nation state and governmental capabilities and responsibilities like war, crime, and espionage frame cybersecurity discussions. This approach largely confines the discussion to the military, intelligence, and law-enforcement communities, which can be secretive by design and sometimes necessity, and can emphasize security while failing to adequately recognize other important democratic principles such as protecting privacy and free association.[45] These intergovernmental efforts also have not proven successful at improving cybersecurity. A more effective approach calls for engaging device manufacturers, software developers, policy advocates, and educational networks to balance equities and empower the public.[46] This type of multistakeholderism encourages transparency, which is needed to overcome the current environment of fear, uncertainty, and doubt ("FUD") bred by the traditional approach to cybersecurity. FUD has proven to be useful at raising awareness about the existence of a threat but less than effective at breeding solutions or

[45] *See* Marília Maciel, Nathalia Foditsch, Luca Belli and Nicolas Castellon,Fundação Getúlio Vargas, *Cybersecurity, Privacy and Trust: Trends*, Fundação Getúlio Vargas, *in Latin America*, *in Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report*, Observatory Cybersecurity in Latin America and the Caribbean (2016), https://publications.iadb.org/bitstream/handle/11319/7449/Cybersecurity-Are-We-Prepared-in-Latin-America-and-Caribbean.pdf?sequence=1&isAllowed=y.

[46] *See, e.g.*, Hans de Bruijn & Marijn Janssen, *Building Cybersecurity Awareness: The need for evidence-based framing strategies*, 34 Gov't Info. Quarterly 1 (Jan. 2017), https://www.sciencedirect.com/science/article/pii/S0740624X17300540; *Cybersecurity Program Should Be More Transparent, Protect Privacy*, Center for Democracy & Tech. (Mar. 30, 2009), https://cdt.org/insight/cybersecurity-program-should-be-more-transparent-protect-privacy/.

improving behavior in the ecosystem.[47] Further, transparent processes that engage the private sector will help to combat efforts by authoritarian regimes and others that use cybersecurity as a cloak to engage in censorship, widespread surveillance, and other actions that counter human rights.

Indeed, a multistakeholder approach can help ensure that network owners and edge providers, among others, have a voice in regulatory efforts, helping to mitigate potential negative impacts to international commerce.[48] Past U.S.-based efforts to develop standards and best practices in cybersecurity, like the NIST-supported Cybersecurity Framework and the DHS, NIST, and NTIA-coordinated effort to produce the Botnet Report have proven the value of a multistakeholder approach. These projects recognized that cybersecurity issues, like automated, distributed attacks, are an ecosystem-wide challenge, and can only be addressed by engaging a broad array of stakeholders.[49]

Assessment

One key lesson from Energy Star is that a system based on self-reported attestations is easily abused. Attestations should be auditable by a third-party observer—either the government, as the program supporting body, or a duly recognized and accredited private entity. In the latter case, the government could provide funding for the audit, or a rebate or other tax incentive for companies that pass muster. As attestation programs scale, the tendency has been for assessments to lose rigor due to rising costs that exert pressure on the market. This tradeoff must be acknowledged, and emphasis should be placed on robust and accountable third-party assessment over rapid scaling.[50]

The EPA and DoE implemented a third-party testing requirement for Energy Star certification after a 2010 Government Accountability Office investigation revealed that the existing system (largely based on self-reported data) was ripe for fraud and abuse.[51] In implementing third-party testing, the EPA relied on the existing ISO/IEC 17065 conformity assessment for product certifying bodies. Companies like MET Labs, Nemco, and Underwriters Laboratory ("UL"), which offer broad and established testing and certification services, were well positioned to provide these services to the EPA, and could be ready to operationalize a cybersecurity labeling scheme. CTIA has already partnered with a number of test labs and

[47] Sam Curry, *Cut the FUD: Why Fear, Uncertainty, and Doubt is harming the security industry*, Helpnetsecurity (Nov. 29, 2017), https://www.helpnetsecurity.com/2017/11/29/fud-cybersecurity/.

[48] *See, e.g.*, Internet Society, *Internet Governance – Why the Multistakeholder Approach Works* (Apr. 26, 2016) https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/.

[49] *See generally*, Botnet Report, *supra* note 7.

[50] *See, e.g.*, Andrew Plato, The Failure of the PCI-DSS? (Feb. 11, 2014), https://www.anitian.com/the-failure-of-the-pci-dss/.

[51] *See* GAO-10-470 (Mar. 2010), https://www.gao.gov/assets/310/301514.pdf.

certifying bodies in order to implement its standard, priming the industry for future cybersecurity requirements.[52]

As a proactive measure, a program manager can provide clear guidance for attestations, defining specific terms and explaining how customers are likely to interpret certain statements. The FTC has long provided this type of information to marketers in the environmental context through its "Green Guides."[53] While compliance with these guides does not foreclose an enforcement action, it does provide a way for marketers to anticipate and avoid practices that might be considered unfair or deceptive.[54]

Attributes

As discussed in other fora, information asymmetries distort the market for consumer IoT.[55] This market failure can be addressed through regulation, such as products liability laws, or in the absence of new regulation, some other mechanism to educate and inform IoT device consumers.[56] Once such mechanism is a voluntary labeling program. Once the decisions of what to assess and how to assess it have been made, three questions arise:

- What should be communicated from the assessment results?
- How should that that be communicated?
- Where should that be communicated?

While some are quick to dismiss trustmarks, arguing that they are an overly simplistic solution to a complex problem, not all labels are created equal. Informational labels come in a variety of formats, and communicate data differently depending on the design, criteria, and even general perception. They can be detailed and technical, as with the traditional Nutrition Facts label on food; they can provide a streamlined rating of key traits, as with the more recent "Facts up Front" labels[57] or they can be simple, trademark-style marks, like the REAL® dairy seal[58] or ENERGY STAR® label. Recently, technology-driven alternative marks like the SmartLabel have entered the market. A cybersecurity mark could take a similar, more dynamic approach to informing IoT device consumers. Devices could, for example, feature a mark that incorporates, or is supplemented by, a QR code linking to more detailed information, similar to the SmartLabel

[52] *See* CTIA, *Certification Resources*, https://www.ctia.org/about-ctia/certification-resources (last visited Jan. 24, 2019).

[53] *See FTC Issues Revised "Green Guides"*, FTC (Oct. 1, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-issues-revised-green-guides.

[54] *See id.*

[55] *See Promoting Stakeholder Actions Against Botnets and Other Automated Threats*, Comments of Public Knowledge, 3-4 (Feb. 12, 2018), https://www.publicknowledge.org/documents/public-knowledge-botnet-comments; *see also* Blythe and Johnson, *supra* note 2 at 4.1.

[56] *See generally*, Benjamin C. Dean, *An Exploration of Strict Products Liability and the Internet of Things* (April 2018), https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

[57] A modified version of the British Guideline Daily Amount (GDA) label, http://www.factsupfront.org/.

[58] http://realseal.com/.

program for information on food and household products.[59] A software bill of materials (SBoM) is another "nutrition label" style solution for providing information on critical pieces of code, which may be unwieldy for standard packaging.[60] Click-through or QR-code access to a SBoM can be a viable solution.

Whatever the format, a cybersecurity label for consumer IoT must provide accessible information to consumers, which enables them to make a meaningful choice. It must be understandable to the average consumer and provide sufficient insight to equip a consumer to make an informed purchase. Given the lack of meaningful metrics and generally sparse consumer education on cybersecurity today, a mark can serve as an appropriate and effective way to reduce the information asymmetries that distort the consumer IoT device market. Problems can arise when a company goes out of business, or a product is circulated in the secondary market. A dynamic label such as a QR code could be a useful tool under these circumstances to inform consumers that the security lifecycle has ended, together with a robust communications strategy by the manufacturer and supported by government engagement, e.g, children's car seats.[61]

A label should be located in a conspicuous place but should not be intrusive to the point that it can interfere with design concept or functionality. Labels that exist on design-oriented products, e.g., the FCC logo on Apple products, tend to be hidden from sight, so care must be taken when considering them as proofs of concept. A label must also be designed to be easily recognized and should be versatile enough to use on a variety of surfaces and materials, for example the tag of soft, connected toy.

Implementation

A government-led Security Shield program will need both legal authority and appropriate funding to properly implement. The program as a whole could find statutory authority under Sections 401 and 501 of the Cybersecurity Enhancement Act of 2014[62] or under Section 103 of the Cybersecurity Information Sharing Act of 2015.[63] Congress should provide Department of Commerce and other appropriate Departments and agencies with additional funds to support their role in such an effort.

Pursuant to the National Technology Transfer and Advancement Act of 1995 (NTTAA) and OMB Circular A-119, a federal agency should in carrying out its mission, where possible,

[59] *See New SmartLabel™ Initiative Gives Consumers Easy Access to Detailed Product Ingredient Information*, GMA (Dec. 2, 2015), https://www.gmaonline.org/news-events/newsroom/new-smartlabel-initiative-gives-consumers-easy-access-to-detailed-ingredien/..

[60] *See* National Telecommunications & Information Administration, *NTIA Launches Initiative to Improve Software Component Transparency*, https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency.

[61] *See, e.g.*, https://www.nhtsa.gov/equipment/car-seats-and-booster-seats.

[62] *See* 15 U.S.C. §§ 7451-61 (requiring NIST to coordinate a national cybersecurity awareness and education program, and to promote the advancement of cybersecurity technical standards).

[63] *See* 6 U.S.C. § 1502 (requiring the heads of appropriate agencies, to distribute information on cybersecurity best practices).

emphasize the use of privately developed consensus standards, where those standards are effective at meeting the agency's needs.[64] The OMB Circular lays out a case-by-case assessment process, and also puts certain limitations on the types of standards federal agencies should prefer—favoring voluntary standards whose development include specific attributes (openness, balance, due process, an appeals process, and consensus).[65] In the absence of such standards, or in cases where the standard in question is for internal use, a government-specific standard is appropriate. It is also important to note that, like Energy Star, a Security Shield program would not necessarily represent a definitive baseline standard for reasonable practices. Security Shield partners should, however, be ahead of the curve and committed to pulling it forward.

Trustmarks can only accomplish their intended tasks if they are legitimate and worthy of public confidence.[66] Driving the Security Shield program through government procurement can signal the kind of approval from a public authority that is necessary to contribute to the mark's legitimacy.[67] As previously discussed, government procurement rules required acquisition of Energy Star products. Congress should consider legislation that would provide similar incentives for a cybersecurity label. Furthermore, additional incentives in the form of tax deductions or rebates as well as reassessment of existing liability limitations are also worthy of discussion in pursuing a label. Assessment costs are significant at scale, and some companies are skeptical of demand for secure-to-market products. Tax incentives at the federal and state levels may be created to overcome this negative inertia. Further, to the extent that it is necessary, tax rebates and deductions for purchases of Security Shield labeled products could encourage consumers to purchase labeled products. It should be noted, however, that consumers are willing to pay for the security and privacy that they value.[68] As with Energy Star, the government can serve to connect businesses to consumers by providing information on participating companies, outlining financing options, and publicly recognizing businesses and organizations that are meeting Security Shield's goals.

Other tools in addition to a label can enhance the effectiveness of the program. These include retail establishments setting minimum security requirements for products they will sell and retail staff trained to inform consumers about security capabilities, to name just two. These steps alone can help, but just as was the case with energy conservation, a label can facilitate additional awareness and thereby additional opportunity to enhance cybersecurity. Short of a full-scale program, retailers such as Amazon, Best Buy, or Walmart working together with manufacturers could undertake a pilot program to assess the viability and effectiveness of a cybersecurity labeling program. The pilot could prioritize products assessed to have better

[64] *See* National Technology Transfer and Advancement Act of 1995, Pub. L. 104-113 §§ 12(d)(1)-(3), 15 U.S.C. § 272; OMB Circular A-119, Revised at 19 (Jan. 22, 2016) ("The Circular does not preclude the use of other standards . . . where use of a [privately developed] standard would not be as effective at meeting the agency's regulatory, procurement or program needs.").

[65] *See* OMB Circular A-119, Revised at 18.

[66] *See* Gilad L. Rosner, *Trustmarks in the Identity Ecosystem*, 22 (Open Identity Exchange, September 1, 2014).

[67] *Id.*

[68] *See, e.g.,* Bruce Brown, *BlackBerry survey: Consumers don't trust connected devices to keep data secure*, Digital Trends (Jan. 7, 2019, 7:00AM), https://www.digitaltrends.com/cars/blackberry-survey-consumers-mistrust-connected-device-security-ces-2019/.

security and should include transparency around the capabilities and assessment leading to such prioritization. In addition, retailers can serve as a resource more generally to consumers about the importance of product security but in doing so should work from a common set of materials developed in partnership with the government and social scientists.

Recommendations

The Security Shield program may be operationalized through a series of discrete steps. Step one is to develop consensus security capabilities baseline or standards. NIST has experience convening multistakeholder processes to develop cybersecurity processes and best practices through its work on the Cybersecurity Framework for Critical Infrastructure and its upcoming IoT Privacy Framework, and could serve as the federal source for the Security Shield labeling program. NIST should facilitate the development of consensus IoT security baseline standards in coordination with the other relevant agencies (e.g., Department of Homeland Security), industry stakeholders, and consumer advocates.

In conjunction with legislative efforts or in advance of them, Step two could be a pilot program. Device manufacturers and the Department of Commerce can and should begin work immediately on a pilot to test the security baseline. A pilot program, for example for routers, printers, baby monitors, or other prevalent government and household products is one way to begin building towards a trusted label that consumers can use to reliably evaluate product risk and move the market towards a more secure internet ecosystem.

Several supporting and enabling efforts are also critical to such a program’s success. These include education and awareness raising, market surveillance, and incentives programs. Each of these efforts requires collaboration between the public and private sectors and would benefit from a single point of focus from the federal government, such as through a program office within the Department of Commerce.