POLICY STRATEGIES TO IMPROVE CYBERSECURITY

VINCENT YESUE*

TABLE OF CONTENTS

I. INTRODUCTION 83
II. ORIGINS AND HISTORY OF CYBERSECURITY INSURANCE 85
A. GOVERNMENT EFFORTS TO DEVELOP THE CYBERSECURITY INSURANCE INDUSTRY AS A POLICY TOOL 87
B. INFORMATION AND STRUCTURAL PROBLEMS 91
C. VICIOUS CYCLE? 92
D. NOT ENOUGH PREMIUMS TO COVER LOSSES? 94
E. THE WORST THREATS AREN'T COVERED? 95
III. A MISSING LEVER: TORTS 96
A. UCC WARRANTY 97
B. NEGLIGENCE LAW 97
C. DESIGN OR MANUFACTURING DEFECTS 98
D. WHY CHANGE TO THE LIABILITY LAW SITUATION IS UNLIKELY TO BE ON THE HORIZON 99
IV. FEDERAL REGULATION 100
V. TAX EXPENDITURES AND DIRECT EXPENDITURES 101
A. EXPENDITURE DESIGN 103
B. OBSTACLES 105
VI. CONCLUSION 109

* Vincent Yesue is an attorney at Rusing Lopez & Lizardi in Tucson, Arizona.

I. INTRODUCTION

Each day, the vulnerability of technology systems to attack and exploitation becomes a more serious threat to our way of life.[1] Every critical part of our daily lives is increasingly enmeshed in networked, computerized systems.[2] Not long ago, using an answering machine, hailing a cab, or going into a bank to withdraw cash would have been plausible scenarios. Today, every step of those errands has been replaced by a form of digital technology and each element touches the public internet.[3] The risks posed by the disruption of the technological systems at the core of today's society are immense and growing.[4] This danger to the common good is being managed ineffectively by private industry,[5] and the government's attempts at risk management have also been unsuccessful.[6] This must change.

The explosive technological growth that has brought us to this point in history can be understood in the context of two concepts at the core of the venture capital-backed technology industry: first-mover advantage and technical debt.

The dynamics of new markets favor the first entrant, especially when the market depends on network effects. Metcalfe's Law suggests that the value of a network is proportional to the square of the number of nodes on the network.[7] The popular interpretation of this law in the marketplace is

---

[1] THE HERITAGE FOUND., *The Growing Threat of Cyberattacks*, https://www.heritage.org/cybersecurity/heritage-explains/the-growing-threat-cyberattacks (last visited May 13, 2022).

[2] KATHLEEN STANSBERRY, JANNA ANDERSON & LEE RAINIE, EXPERTS OPTIMISTIC ABOUT THE NEXT 50 YEARS OF DIGITAL LIFE 55–58 (Pew Rsch. Ctr. 2019).

[3] COLLEEN MCCLAIN, EMILY A. VOGELS, ANDREW PERRIN, STELLA SECHOPOULOUS & LEE RAINIE, THE INTERNET AND THE PANDEMIC, (Pew Rsch. Ctr. 2021).

[4] *A Guide to Cyber Risk*, ALLIANZ GLOB. CORP. & SPECIALTY (Sept. 2015), https://www.agcs.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html.

[5] Amitai Etzioni, *Private Sector Neglects Cyber Security*, NAT'L INTEREST, (Nov. 29, 2011), https://nationalinterest.org/commentary/private-sector-neglects-cyber-security-6196.

[6] Jody R. Westby, *The Government Shouldn't be Lecturing Private Sector on Cybersecurity*, FORBES, (June 15, 2015, 02:05pm), https://www.forbes.com/sites/jodywestby/2015/06/15/the-government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity/?sh=6e481ced621b.

[7] Margaret Rouse, *Metcalfe's Law*, TECHOPEDIA (May 28, 2019), https://www.techopedia.com/definition/29066/metcalfes-law.

that a product that finds even a small audience may develop a virtually insurmountable advantage over the next entrant to the same market.[8]

The perceived advantage accrued by the first mover puts significant economic pressure on market entrants to forego thorough development of every feature of a new technology product and, instead, to enter the market with the least complete version of the technology that could possibly be acceptable to early adopters. This phenomenon is so pervasive that it has not only a name but also an acronym: the minimum viable product (MVP).[9] It is not difficult to imagine a scenario in which an entrant to a new technology market creates an MVP without sufficient thought to security architecture.[10] The product could enter the market with severe security vulnerabilities that remain latent[11] until discovered either by a well-meaning researcher or an attacker.[12] The manufacturer could choose to remediate these vulnerabilities in a subsequent release, but even then, sufficient incentive or opportunity may not exist.[13] The built-in technical shortcomings of a product, left behind for commercial reasons are known as technical debt.[14] Someday, technical debt will come due, either because the built-in shortcomings need to be fixed to continue to develop the

---

[8] While some disagree on the effectiveness of first-mover advantage or the circumstances under which it is a real advantage, the general consensus is that the first to market has an advantage. *See e.g.*, Fernando F. Suarez & Gianvito Lanzolla, *The Half-Truth of First-Mover Advantage*, HARV. BUS. REV. (Apr. 2005), https://hbr.org/2005/04/the-half-truth-of-first-mover-advantage.

[9] *See generally* ERIC RIES, THE LEAN STARTUP: HOW CONSTANT INNOVATION CREATES RADICALLY SUCCESSFUL BUSINESSES (2011) (discussing the use of MVPs in the entrepreneurial and start-up space). *See also* Maksym Babych, *A Review of the Minimum Viable Product Approach*, FORBES, (Dec 8, 2021, 07:00 AM), https://www.forbes.com/sites/theyec/2021/12/08/a-review-of-the-minimum-viable-product-approach/?sh=40c478702e20 (stating that MVP is a term coined by Frank Robinson and highlighting MVP as a popular test of business models in prospective start-up launches).

[10] Nicole Perrault, *Minimum Viable Product and Its Impact on Cybersecurity*, DOVER MICROSYSTEMS (Oct. 4, 2017), https://info.dovermicrosystems.com/blog/mvp-cybersecurity-impact.

[11] *Id.*

[12] *Vulnerability*, F-SECURE, https://www.f-secure.com/v-descs/articles/vulnerability.shtml (last visited May 13, 2022).

[13] Perrault, *supra* note 10.

[14] The term is commonly attributed to Ward Cunningham, developer of the first wiki software. *See e.g.*, Martin Fowler, *TechnicalDebt*, MARTINFOWLER.COM (May 21, 2019), https://martinfowler.com/bliki/TechnicalDebt.html. *See also* Dan Radigan, *Escaping the Black Hole of Technical Debt*, ATLASSIAN, https://www.atlassian.com/agile/software-development/technical-debt (last visited May 13, 2022).

product or because the shortcomings have been used by attackers to gain an advantage over users of the product.[15] We return to this example in the discussion of tax policy near the end of this paper, after a discussion of the development of policy tools that have been deployed to improve the nation's cybersecurity posture.[16]

These efforts can be categorized according to several methodologies: cybersecurity insurance, tort law, federal regulation, and taxation policy. Historically, policy efforts have focused on cybersecurity insurance to the exclusion of the rest. This paper analyzes each in turn and concludes with a discussion of the most useful changes that could move the needle toward a more secure society.

II. ORIGINS AND HISTORY OF CYBERSECURITY INSURANCE

Cybersecurity insurance originated as a mechanism for organizations to protect against technology-related losses excluded by commercial general liability insurance.[17] The efforts of the Bush 43 and Obama administrations adopted cybersecurity insurance as part of a policy to develop and incentivize cybersecurity best practices.[18] The federal government's objective of ameliorating the national security problem rooted in insecure computers and networks has not come to pass. Instead of revolutionizing cybersecurity practices, this insufficiently capitalized insurance line suffers from information asymmetry between insurers and insureds and creates a perverse incentive for online organizations to remain insecure. Unfortunately, this insecurity serves as a deep well of money from which international criminal gangs can fund and improve the capacity of their illegal operations.

---

[15] Jeff Atwood, *Paying Down Your Technical Debt*, CODING HORROR, (Feb. 27, 2009), https://blog.codinghorror.com/paying-down-your-technical-debt/ (stating that "accruing technical debt is unavoidable"). *But cf.* Michael Engstler, *The Vulnerability Debt in Product Security*, FORBES, (Sept. 30, 2021, 08:15 AM), https://www.forbes.com/sites/forbestechcouncil/2021/09/30/the-vulnerability-debt-in-product-security/?sh=299d94232d62 (stating that "[c]yber risk and software vulnerabilities are often perceived as purely technical . . . [h]owever, that should not be the case").

[16] *See supra* Section 5.

[17] DANIEL HANKINS, ADVANCED GOV'T L., ch. 3, § VI (2020).

[18] *See Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2022*, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited Nov. 8, 2023); *see also* Juliana De Groot, *The History of Data Breaches*, DIGIT. GUARDIAN, (Aug. 22, 2022), https://www.digitalguardian.com/blog/history-data-breaches.

Throughout the development of the commercial insurance industry in America, cybersecurity risk was not a major consideration because computers were not yet in widespread use. As computers became more ubiquitous in American business, cyber losses that arose might have been covered under an all-risk property policy or excluded because they were not a named peril.[19] But, as the risks increased with the advent of the consumer internet and the sophistication of hackers, insurance companies realized that the risk needed to be separated from general commercial risks.[20] As such, insurers began to exclude cyber risk from the general policies.[21]

By 1997, an Atlanta, Georgia, agent named Steven Haase was working with clients who had significant risk exposure, including early internet banks and cybersecurity providers.[22] Mr. Haase saw the amount of exposure that lay beyond the protection of the existing insurance lines that his customers bought.[23] His clients and their risk profiles, coupled with the exclusion of cybersecurity risk from general policies led Mr. Haase to design a product with AIG to help manage risk.[24] This might have been the first cybersecurity insurance product.[25] At the outset, the policies that Haase called "cyber liability policies" covered the deletion of online data or data processing errors.[26] It was not until the early 2000s that cyberattacks and security breaches were covered.[27] However, insider threats and losses due to regulator fines were specifically excluded, and coverage was limited to damages relating to third parties.[28] But by the mid-2000s, modern first-party policies entered the market.[29] These newer policies covered business interruption due to cyberattacks, ransomware extortion, and damage to network assets.[30] California led states in creating statutory consumer

---

[19] PHILIP L. BRUNER & PATRICK J. O'CONNOR, JR., BRUNER & O'CONNOR ON CONSTR. L., § 11:418, n. 11 (2023).

[20] HANKINS, *supra* note 17.

[21] *Id*.

[22] Andrea Wells, *What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now*, INS. J., (Mar. 1, 2018), https://www.insurancejournal.com/news/national/2018/03/01/481886.htm.

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *The Evolution of Cyber Insurance*, PROWRITERS, https://prowritersins.com/cyber-insurance-blog/cyber-insurance/ (last visited May 13, 2022).

[27] Wells, *supra* note 22; *The Evolution of Cyber Insurance*, *supra* note 26.

[28] *The Evolution of Cyber Insurance*, *supra* note 26.

[29] *Id.*

[30] *Id.*

protections for consumers who were caught up in cyberattacks with the California Security Breach and Information Act,[31] mandating breach notification and requiring insurers to offer coverage that protected insureds against the costs of notifying consumers and defending brand value in the court of public opinion after highly-publicized breaches.[32]

A. GOVERNMENT EFFORTS TO DEVELOP THE CYBERSECURITY INSURANCE INDUSTRY AS A POLICY TOOL

Since the early 2000s, the federal government has urged the development of the cybersecurity insurance industry as a necessary part of bolstering national security by leveraging insurance risk rating to improve the security of computer software and systems.[33] In 2002, the Bush administration met with industry leaders to help clear the regulatory path for more cybersecurity insurance policies.[34] Brian Krebs[35] described the Bush administration's efforts to expand cybersecurity insurance as a strategy similar to the development of fire insurance in the early 1900s, which drove increased scrutiny on fire prevention and led to increased safety.[36] The idea was that as the internet became more hostile and as losses to American companies began to mount, more companies would seek cybersecurity insurance.[37] Insurers would partner with industry experts and encourage insureds to adopt sound preventative cybersecurity practices and remediation strategies to achieve low-risk ratings and decrease premiums.[38] Insurance industry insiders predicted that cybersecurity insurance would become similar to other kinds of insurance, that companies would consider it a necessary cost of doing business, and that the market could "reach $2.5 billion in premiums by 2005."[39]

---

[31] CAL. CIV. CODE § 1798.29(a) (agency); CAL CIV. CODE § 1798.82(a) (person or business).

[32] *The Evolution of Cyber Insurance*, *supra* note 26.

[33] Brian Krebs, *White House Pushing Cybersecurity Insurance,* WASH. POST (June 27, 2002, 1:35 PM), [https://seclists.org/politech/2002/Jul/21].

[34] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, THE NAT'L STRATEGY TO SECURE CYBERSPACE (2003).

[35] At the time, Krebs was a Washington Post staff writer and later, the proprietor of KrebsOnSecurity, an "in-depth security news and investigation" blog. *See generally About the Author*, KREBSONSECURITY, https://krebsonsecurity.com/about/ (last visited Nov. 8, 2023).

[36] Krebs, *supra* note 33.

[37] *Id.*

[38] *Id.*

[39] *Id.*

By 2010, the bipartisan Cybersecurity Act of 2010 was introduced to the Senate with a provision calling for the Obama administration to "encourage a market for cybersecurity insurance to protect businesses."[40] The bill did not pass.[41] Nevertheless, the White House took up the Senate's advice and in February 2013, promulgated Executive Order 13636, which addressed the growing "cyber threat to critical infrastructure" and directed executive branch agencies to respond to the threat.[42] Notably, the National Institute for Science and Technology was directed to develop the Cybersecurity Framework—"a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[43] The same Executive Order directed the Departments of Homeland Security, Commerce and the Treasury to "coordinate establishment of a set of incentives designed to promote participation in the Program [to support the Cybersecurity Framework's adoption]" and to "[analyze] the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program."[44] When the Department of Commerce (through the National Telecommunications and Information Administration (NTIA)) responded to President Obama with a list of steps the U.S. Government could take "to build a successful incentives structure," the first suggestion was to engage the insurance industry.[45] NTIA's logic echoed that of the Bush 43 administration: the insurance industry was accustomed to evaluating preventative measures, they were used to pricing risk, and they were used to deploying underwriting practices that could encourage the adoption of the risk-reducing preventative measures.[46]

The Department of Homeland Security's (DHS) response to the Executive Order was mixed. DHS assessed that insurance could serve as a

---

[40] Erich Schwartzel, *Cybersecurity Insurance: Many Companies Continue to Ignore the Issue*, PITTSBURGH POST-GAZETTE, (June 22, 2010, 4:00 AM), https://www.post-gazette.com/business/tech-news/2010/06/22/Cybersecurity-insurance-Many-companies-continue-to-ignore-the-issue/stories/201006220157; S. 773, 111th Cong. (2010).

[41] S. 773.

[42] Exec. Order No. 13636, 78 Fed. Reg. 11739 § 1 (Feb. 12, 2013).

[43] *Id.* § 7.

[44] *Id.* § 8.

[45] NAT'L TELECOMM. & INFO. ADMIN., DEP'T OF COM., DISCUSSION OF RECOMMENDATIONS TO THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS TO JOIN A VOLUNTARY CYBERSECURITY PROGRAM, at 1 (2013).

[46] *Id. See also* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 36.

"benefit that motivates a decision or action by critical infrastructure asset owners and operators to adopt the Cybersecurity Framework under development by NIST."[47] DHS also suggested a federal reinsurance program to backstop the development of commercial cybersecurity insurance policies.[48] Additionally, DHS identified problems with the insurance-as-incentive approach: first, if insureds believed they were protected, they might engage in riskier behavior (an example of the concept of moral hazard); second, it would be difficult for insurance companies to compute damages associated with a cyber loss; and third, insurers would be hesitant to insure acts of terrorism or acts of war, both of which were kinds of threats that were on the federal government's radar.[49] DHS was unable to conclude that cybersecurity insurance could effectively influence the behavior of U.S. organizations.[50]

The response to the Executive Order made by the Department of the Treasury was pointedly negative with respect to cybersecurity insurance. Echoing DHS, the Treasury identified the moral hazard problem but also noted the information asymmetry between insurers, who know relatively little about the cybersecurity hygiene of their insureds, compared to the in-depth knowledge that the insureds have about their own security practices.[51] On the other hand, it might be the case that the problem isn't an information asymmetry so much as a lack of loss data from the insurer's perspective.[52] The NTIA reported that Commerce's Notice of Inquiry responses included a skeptical take from the American Insurance Association because the "continued advancements in the cyber insurance market will depend on access to sufficient loss data and a knowledgeable workforce that stays current with changing technologies and threats."[53] The Treasury also noted that in 2012, while it was difficult to put an exact number on the size of the cybersecurity insurance market, "some private estimates put annual gross written premiums in the $1 billion range," out of a total of about $247 billion in annual premiums across all commercial

---

[47] DEP'T OF HOMELAND SEC. INTEGRATED TASK FORCE, EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 5 (2013), https://www.cisa.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

[48] *Id.* at 7.

[49] *Id.* at 29.

[50] *Id.* at 12–13.

[51] DEP'T OF THE TREASURY, TREASURY DEPARTMENT REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, at 23 (2013).

[52] Krebs, *supra* note 33.

[53] Letter from Angela Gleason, Assoc. Couns., Am. Ins. Ass'n, to cyberincentives@ntia.doc.gov (Apr. 29, 2013) (on file with author).

lines in the United States.[54] This represents a far cry from the 2002 prediction for the year 2005 of $2.5 billion even eight years after 2005 came and went.

Nevertheless, the cybersecurity insurance train rolled on. In February 2014, the National Institute for Science and Technology announced the Cybersecurity Framework, which did not itself include explicit guidance as to the incentives to be used.[55] However, the message sent by the White House was clear, as relayed by a Senior Administration Official in a briefing on the launch of the Cybersecurity Framework:

> "[W]e believe that the best drivers for adoption or use of the framework will ultimately be market based. Don't get me wrong, I think the government-based incentives are really important for us to pursue. But at the end of the day, it's the market that's got to drive the business case for the Cybersecurity Framework. The federal government is going to do its best to make the costs of using the framework lower, and the benefits of the framework higher, but it's the market that's going to ultimately make this work."[56]

Later that same month, industry analysts reported an uptick in company purchases of data breach insurance, suggesting that the government's multi-pronged effort to drive the industry forward was beginning to bear fruit—or at least, was an idea whose time had come.[57]

---

[54] NAT'L TELECOMM. & INFO. ADMIN., DEP'T OF COM., *supra* note 47 (citing Sasha Romanosky, *Comments to the Department of Commerce on Incentives to Adopt Improved Cybersecurity Practices*, INFO. L. INST., at 6 (Apr. 26, 2013) (stating NTIA gave a similar estimate, citing an estimate "that current, total annual cybersecurity insurance purchases range[s] from $500 million to $1 billion.").

[55] *See generally* NAT'L INST. OF STANDARDS AND TECH., DEP'T OF COM., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014).

[56] Press Release, Off. of the Press Sec'y, Background Briefing on the Launch of the Cybersecurity Framework (Feb. 12, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/02/12/background-briefing-launch-cybersecurity-framework.

[57] Deirdre Fernandes, *More Firms Buying Insurance for Data Breaches*, THE BOS. GLOBE, (Feb. 17, 2014, 12:00 AM), https://www.bostonglobe.com/business/2014/02/17/more-companies-buying-insurance-against-hackers-and-privacy-breaches/9qYrvlhskcoPEs5b4ch3PP/story.html. Note that this article presents a different timeline of the exclusion of cyber risks from commercial general liability products than the one presented in Krebs *supra* note 33.

Today, cybersecurity risks are sharply increasing, with the recent pandemic-driven trends toward online work and the increased visibility of attacks, causing both an uptick in demand for cybersecurity insurance and predictions of price hikes in the coming years.[58] A poll undertaken by one insurance company and published in their 2021 report found twenty-seven percent of firms had standalone cybersecurity insurance,[59] while another company recorded that 200 cybersecurity insurance providers in the U.S. collected $2.74 billion in premiums in 2020.[60]

B. INFORMATION AND STRUCTURAL PROBLEMS

Some immediate problems with the cybersecurity insurance industry center on pricing as it relates to the insurance companies' access to information and market demand. An information asymmetry exists between consumers, who know how risky their systems are, and insurers, who don't, or at the very least, an information gap exists on the side of the insurer, who does not have sufficient loss data to calculate risk.[61] This makes it challenging for insurance companies to set prices that reflect the risk that they are taking on.[62] Insurers can have a difficult time estimating how long a breach might last, which causes additional pricing problems.[63] Because of the high-profile nature of cyberattacks, pricing can be dynamic. Prices have fallen when additional insurers have entered the marketplace,[64] but they

---

[58] L.S. Howard, *Re/Insurance Cyber Rates Could Double Before 2023, as Attacks Skyrocket: S&P*, INS. J., (Sept. 30, 2021), https://www.insurancejournal.com/news/international/2021/09/30/634535.htm.

[59] HISCOX CYBER READINESS REPORT 2021, HISCOX 3 (2021) https://www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf.

[60] U.S. CYBER MARKET UPDATE, AON (2021), http://thoughtleadership.aon.com/Documents/20210609-2021-cyber-market-update.pdf (follow hyperlink, then scroll down to June 09, 2021 U.S. Cyber Market Update, click on it, and submit information request to obtain report).

[61] DEP'T OF THE TREASURY, *supra* note 53, at 6–7.

[62] Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 222 n.210 (2017) (citing Adam F. Scales, *A Nation of Policyholders: Governmental and Market Failure in Flood Insurance*, 26 MISS. C.L. REV. 3, 8 (2006) stating "Without reasonably accurate data to generate loss predictions, insurance cannot be correctly priced.")).

[63] Thomas D. Hunt, *"The Internet of Buildings": Insurance of Cyber Risks for Commercial Real Estate*, 71 OKLA. L. REV. 397, 409 (2019).

[64] SAM CARTER & MICHAEL MAINELLI, CYBER-CATASTROPHE INSURANCE-LINKED SECURITIES ON SMART LEDGERS 39 (2018).

have risen after high-profile breaches. [65] Now, with insured losses sharply increasing and loss ratios following suit, profits are down at a time when demand is rising.[66] Cybersecurity insurance policies are also extremely complex, sometimes causing the insured to misunderstand what risks are being insured.[67] But even aside from these challenges, there are deep structural problems with the nature of cybersecurity as it exists today.

C. VICIOUS CYCLE?

One structural problem might be that cybersecurity insurance itself is driving cyber risk. Organizations, cognizant of regulation, contractual requirements, and the fact that the internet comprises a huge share of their risk exposure, purchase insurance against this risk.[68] Whether or not the moral hazard problem identified by the Treasury and others as far back as the response to Executive Order 13636 in 2013 —that insureds might purchase coverage and then ignore the risks—it may be the case that companies, which only have so much money to spend on cybersecurity, might be motivated to buy cybersecurity insurance and then skip the critical step of implementing security best practices, leaving themselves covered but vulnerable to attack.[69] This is the best-case scenario for a criminal ransomware gang.

Ransomware is a complex topic, but in simple terms, the scam works like this: (1) an attacker finds a vulnerable victim with a computer that can be manipulated; (2) the attacker manipulates the system in a way adverse to the victim's interest (e.g., encrypts files to inconvenience the victim, displays a pornographic image to embarrass the victim, or locks the computer to make it unusable to the victim); (3) the attacker provides the victim with a means to pay to end the attack; and (4) the attacker waits to

---

[65] Arielle Waldman, *Cyber Insurance Premiums, Costs Skyrocket as Attacks Surge*, TECHTARGET (Oct. 11, 2021), https://www.techtarget.com/searchsecurity/news/252507932/Cyber-insurance-premiums-costs-skyrocket-as-attacks-surge.

[66] Howard, *supra* note 58.

[67] Booz Allen Hamilton, *How to Not Pay a Ransom*, AM. BAR ASS'N (2022), https://www.americanbar.org/content/dam/aba/administrative/tips/programs/cyber-2022-materials/materials/cyberthursday-materials.pdf.

[68] Toby L. Merrill, *Cyber Liability Market is Older, Wiser, Smarter and Still Growing*, INS. J., (Jan. 29, 2007), https://www.insurancejournal.com/magazines/mag-features/2007/01/29/76734.htm.

[69] Liam M.D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1, 5 (2014).

see if the victim will pay. [70] In short, ransomware is extortion using a computer.[71] The attack relies upon a simple, untraceable, unreversible means by which the victim can pay the attacker, which historically meant prepaid electronic systems.[72] The explosion of cryptocurrency has driven a great deal of ransomware activity toward this payment method.[73] Either way, though, what the ransomware attacker needs is a victim with both a vulnerable computer and the means to pay a ransom to get the attack to end: this is exactly the case when an organization spends the bulk of its cybersecurity budget on cybersecurity insurance while subsequently failing to take cybersecurity precautions to reduce their risk of attack. This likely is why ransomware is becoming increasingly more common and why it has evolved from attacks against individuals (i.e., "we saw you looking at porn, pay $200 or we will tell everyone") to an attack against huge corporations (e.g., Garmin,[74] Colonial Pipeline[75]).

As a result, some insurers "have either reduced how much cyber they'll write or have pulled out of the market entirely."[76] Instead of what was envisioned when the White House began to throw its weight behind the concept of cybersecurity insurance as a solution to the national security problem posed by insecure computers, cybersecurity insurance has become the funding source for increasingly sophisticated cyberattacks.[77] This failure suggests that insurance might not be the best mechanism to drive behavioral change in the cybersecurity arena.

---

[70] GAVIN O'GORMAN & GEOFF MCDONALD, RANSOMWARE: A GROWING MENACE 2 (2012).

[71] *Id.*

[72] *Id.* at 4.

[73] Greg Myre, *How Bitcoin Has Fueled Ransomware,* NPR (June 10, 2021, 5:06 AM), https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks.

[74] Catalin Cimpanu, *Hacker Gang Behind Garmin Attack Doesn't Have a History of Stealing User Data,* ZDNET (July 28, 2020, 1:59 PM), https://www.zdnet.com/article/hacker-gang-behind-garmin-attack-doesnt-have-a-history-of-stealing-user-data/.

[75] William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 3:58 PM) https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

[76] Tom Johansmeyer, *The Cyber Insurance Market Needs More Money*, HARV. BUS. REV. (Mar. 10, 2022), https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money.

[77] *See generally* Matt Smith, *How Insurers Play a Big Role in Spurring Cybercrime*, BARRON'S (Oct. 3, 2021, 7:50 PM), https://www.barrons.com/articles/ransomware-attack-cyber-insurance-industry-51633075202.

D. NOT ENOUGH PREMIUMS TO COVER LOSSES?

There might not be enough money in the industry to cover the losses that will be suffered. The risks to insurance companies are increasing as attackers get better at attacking, victims get less averse to paying ransoms, and the world generally gets less predictable.[78] A UK cybersecurity insurance company estimated that in 2018, total cybersecurity-related losses were about $1.2 billion, a number that increased fifty percent year-on-year to an estimated $1.8 billion in 2019.[79] This drives growth in the number of policies written.[80] Demand and increased risk are two factors that squeeze the insurer, and the wild card is the fact that insurers do not have sufficient data about past attacks to truly understand the risk.[81]

As of January 2021, the math is simple: at the very high end of the cybersecurity insurance market, there are about 250 companies that have purchased insurance worth $200 million or more.[82] The premiums that these companies pay are estimated to be about twenty percent of the $5 billion global total premiums paid, approximately $1.1 billion.[83] If there were five insured losses slightly in excess of $200 million this year,[84] they would account for all of the premiums collected, and it would represent a compromise of just two percent of the insured "big fish."[85] The numbers don't look too different for companies that buy more or less than $200 million worth of insurance, and the situation is the same: a shockingly small percentage of successful attacks resulting in complete payouts could drive insurance company profits into the ground.[86]

---

[78] Tom Johansmeyer, *Cybersecurity Insurance has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.

[79] HISCOX CYBER READINESS REPORT 2020, HISCOX 2 (2020) https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF.

[80] *Id.* at 16.

[81] *See generally id.*

[82] Jonahsmeyer, *supra* note 78.

[83] *Id*.

[84] *Id.*

[85] *Id.*

[86] *Id*. ("[T]hink about companies with at least $500 million in protection . . . . [T]wo total losses could wipe out a year's premium. Insurers might have to wait half a century to earn enough premium against those losses. Even for companies buying $100-199 million in premium, the exposure is significant . . . . It would only take a handful of losses wipe out the $1.44 billion in premium they generate.").

E. THE WORST THREATS AREN'T COVERED?

Policy exclusions denying coverage to losses resulting from acts of war are not novel.[87] Recently, though, the concept of "hybrid war" has introduced a sense of uncertainty as to the boundaries of traditional "kinetic" warfare and competitive, inter-state activity in cyberspace.[88] From one perspective, competitive activities like those Russia undertook in its 2008 incursion into Georgia[89] "may not clearly cross the threshold of war . . . [perhaps] due to the ambiguity of international law, ambiguity of actions and attribution, or because the impact of the activities does not justify a response."[90] But in November 2021, Lloyd's Market Association released a set of four newly drafted War, Cyber War and Cyber Operation Exclusions possibly in recognition of the fact that traditional acts of war exclusions were not specific enough in light of the uncertainty around how and when cyberattacks might rise to the level of war.[91] Whether or not a certain cyberattack fulfills the criteria for an act of war under international humanitarian law, Lloyd's seeks to clarify the character of cyber operations that are excluded from cybersecurity insurance policies (and which, presumably, would require war risk insurance for coverage to be present).[92] The four exclusions "are models for use in standalone cyber insurance policies" that present a range of options for insurers writing policies.[93] The first is extremely broad, bringing a form of "cyber operations," defined as "the use of a computer system by or on behalf of a state to disrupt, deny, degrade, manipulate or destroy information in a computer system of or in

---

[87] *Fifth Public Hearing of the National Commission on Terrorist Attacks Upon the United States* (2003) (statement of John Degnan, Vice Chairman, Chubb Corporation) (explaining Chubb's response in the days after 9/11, during which the applicability of the war exclusion to the 9/11 terrorist attacks on the United States was considered; Chubb ultimately decided to pay these claims).

[88] Andrew Dowse & Sascha-Dominik (Dov) Bachmann, *Explainer: What is 'Hybrid Warfare' and What is Meant by the 'Grey Zone'?*, THE CONVERSATION (June 17, 2019, 4:35 AM), https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841.

[89] Sarah P. White, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*, MODERN WAR INST. AT W. POINT (Mar. 20, 2018), https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/.

[90] Dowse & Bachmann, *supra* note 88.

[91] Vincent J. Vitkowsky, *Briefing Note on the New LMA War, Cyber War and Cyber Operation Exclusions for Cyber Insurance Policies*, GFELLER LAURIE, LLP 1, 2–3 (2021), https://www.gllawgroup.com/wp-content/uploads/2021/12/LMA-Cyber-War-and-Cy-Op-Exclns.pdf (internal citation omitted).

[92] *Id.* at 2.

[93] *Id.* at 1.

another state," within the definition of war.[94] This is probably consistent with the international law of armed conflict.[95] The other exclusions deny coverage where the loss is "directly or indirectly occasioned by, happening through or in consequence of war or a cyber operation carried out in the course of war."[96] Again, while an actual war is required, it is not necessarily required that the cyber operation has a kinetic effect in order for its effects to be excluded— consistent with the law of international armed conflict.[97] Lloyd's changes, taking place during Russia's preparations to intensify the 2014 conflict against Ukraine, made even more sense after January 2022, when cyberattacks degraded not only Ukraine's public and financial sectors, but also technology systems worldwide.[98]

If these exclusions become widespread in cybersecurity insurance policies, the risk to policyholders increases because the definition of acts of war becomes much broader.[99]

III. A MISSING LEVER: TORTS

Perhaps the most challenging problem related to cybersecurity insurance is the fact that federal policy puts most of its eggs in the insurance basket, to the exclusion of other mechanisms of control traditionally used to nudge industries in the direction of improved safety. It is not particularly surprising, given the attendance of insurance industry representatives—but not class-action plaintiffs' lawyers—during the Obama administration's policy discussions, that the shortcoming of negligence law as it applies to insecure software was not addressed by the policy. That shortcoming is the extreme difficulty, if not impossibility, under current law, to subject the technology industry to UCC warranty law,

---

[94] *Id.* at 2.

[95] Michael N. Schmitt, *The Law of Cyber Targeting*, 68 NAVAL WAR COLL. REV. 11, 16–17 (2015) (Schmitt, Director of the Tallinn Project, notes that it is likely that even cyber operations without physical effects could be considered "attacks" under the Geneva Conventions Additional Protocol I. While it is unlikely that data could be considered an object of an attack given that "object" is defined by tangibility in GC-AP I, "a majority of experts involved in the Tallinn Project" would interpret "loss of functionality" of a digital system within the scope of damage to that system, even if the system was still physically intact.).

[96] Vitkowsky, *supra* note 91, at 3 (internal citation omitted).

[97] Schmitt, *supra* note 95.

[98] *Key Market Forces Influencing the Risk*, LLOYD'S (July 2022), https://www.lloyds.com/news-and-insights/futureset/futureset-insights/ukraine-a-conflict-that-changed-the-world/market-forces.

[99] *See* U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY INS. WORKSHOP READOUT REP. 13–14 (2012).

to liability law for negligence, or to product liability law for defective design or manufacture of software.

A. UCC WARRANTY

If a plaintiff suffering damages from cybersecurity risk wants to sue under a UCC breach-of-warranty suit, several conditions need to be met. At the outset, the software must be determined to be a "good" under the UCC.[100] Courts are generally likely to make such a determination, but if they do not, the UCC does not apply.[101] Once this hurdle is passed, three options allow for recovery: (1) a drafting error in the manufacturer's limitation of liability clause; (2) manufacturer claims being disclaimed in a manner found to be unconscionable; or (3) manufacturer claims being disclaimed in a manner other than one found to be unconscionable, but either with privity or in a jurisdiction that does not require privity to exist in order to sustain such a suit.[102] Because no reasonable manufacturer of software would be likely to allow such a defective agreement to attach to their software, UCC warranty suits are extremely unlikely to help a consumer who suffers damages from insecure software.

B. NEGLIGENCE LAW

On the other hand, if a plaintiff wants to sue a software manufacturer on a theory of general liability, different conditions need to be satisfied. First, a duty of care needs to be established. Surprisingly, software providers are frequently found to lack a duty to design and develop secure software, and they are frequently found to lack the duty to instruct the user on what dangers are present and how to use the software safely.[103] There isn't a uniform standard of care across states.[104] Second, whether or not there has been a breach of the software provider's duty must be established, but in addition to the questionable status of the software manufacturer's duty, no standard test exists to determine whether this is the case.[105] Third, proximate causation must be shown, but in almost any imaginable situation where damages result, intervening or superseding fault exists on the part of either the user or a criminal third party. Very rarely is

---

[100] Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?* 67 MD. L. REV. 425, 435, n.70 (2008).

[101] *Id.*

[102] *Id.* at 438–39.

[103] *Id.* at 442–44.

[104] *Id.* at 444.

[105] *Id.* at 447.

the software itself at direct fault.[106] While the fact that damages result from a breach is often obvious, the amount of those damages can be difficult to quantify.[107] More importantly, not all states allow economic damages in negligence claims, and none allow punitive damages absent gross negligence.[108] Accordingly, there are plenty of obstacles that make it difficult for a plaintiff to sue a software manufacturer on a theory of negligence after a cybersecurity incident.

C. DESIGN OR MANUFACTURING DEFECTS

A plaintiff who wants to sue a software manufacturer on a theory of defective design or manufacture runs into a fork in the road. Defective design is another way of talking about negligence analysis, so in this case, the plaintiff must refer to the previous subsection for guidance.[109] Defective products are a different story, since they present strict liability. If software can be said to be defective by manufacture, not design, then there is, at first glance, a direct path to plaintiff recovery.[110]

Upon further inspection, though, there are two problems. First, although software is classified under the UCC as a "good," under defective product manufacture law, the precedent is that software is not a product due to its intangibility.[111] If a court takes this point of view, it is a complete bar to a defective product manufacturing suit.[112] Second, from the software providers' point of view, the principal argument would be made that the design process for software is never complete.[113] In the modern software development life cycle, software is continually being "designed," whereby product managers, technology architects, and individual developers continually make implementation choices—even customers are involved in the continuous process of designing and redesigning software.[114] If we acknowledge the reality of the modern software industry that the design process never ends until the software is obsolete, then any liability is solely

---

[106] *Id.* at 442, 448–49.
[107] *Id.* at 449–50.
[108] *Id.*
[109] *Id.* at 467–68.
[110] *Id.* at 461, n. 215.
[111] *Id.* at 462.
[112] *Id.* at 470.
[113] Personal experience and conversations with several experienced security practitioners and software design lifecycle experts. *See also* discussion *infra* Section 5.b (describing the design and development lifecycle of Boeing 737 and Microsoft Windows).
[114] *See* discussion *infra* Section 5.b.

in the realm of product defect and, therefore, subject to all the limitations of negligence described above.

D. WHY CHANGE TO THE LIABILITY LAW SITUATION IS UNLIKELY TO BE ON THE HORIZON

To hold software manufacturers responsible for damage that results from their insecure software, some have called for federal law to address the gap and provide a mechanism by which to use liability law.[115] The software industry fights the prospect of product liability, arguing that money spent on lawsuits is money not spent on improving the state of their software.[116] Even if the software industry accepted such legislation—perhaps as part of a bargain whereby they took responsibility for their shortcomings in exchange for tax breaks when they followed best practices—it seems unlikely that Congress could pass sweeping technology reform legislation when the political system appears dysfunctional and much of the reform movement oxygen is taken up by Section 230 and antitrust concerns.[117] Moreover, the changing landscape of Congress, marked by political polarization and shifting priorities, further diminishes the prospects of enacting sweeping technology reform. With the political agenda during the relevant years preoccupied by military conflict, financial turmoil, and the future of democracy, finding consensus on comprehensive legislation addressing software liability becomes even more challenging amidst the evolving dynamics of legislative priorities.

---

[115] COMPUT. SCI. & TELECOMMS. BD., DIV. ON ENG'G & PHYSICAL SCIS. & NAT'L RSCH. COUNCIL, CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 14 (Nat'l Academy Press 2002).

[116] *S. 96, the Y2K Act: Hearing before the Comm. on Commerce, Sci., and Transp.*, 106th Cong. 67 (1999) (statement of Robert W. Holleyman II, President and CEO, Business Software Alliance).

[117] *See generally* Sarah A. Binder, *Going Nowhere: A Gridlocked Congress*, BROOKINGS (Dec. 1, 2000), https://www.brookings.edu/articles/going-nowhere-a-gridlocked-congress/; Daren Bakst & Dustin Carmack, *Section 230 Reform: Left and Right Want It, for Very Different Reasons*, THE HERITAGE FOUND. (Apr. 12, 2021), https://www.heritage.org/technology/commentary/section-230-reform-left-and-right-want-it-very-different-reasons; Diane Bartz, *Big Tech to Face Another Bipartisan U.S. Antitrust Bill*, REUTERS (Oct. 14, 2021, 6:37 PM), https://www.reuters.com/world/us/big-tech-face-another-bipartisan-antitrust-bill-2021-10-14/.

IV. FEDERAL REGULATION

A second mechanism that could be used to control the national cybersecurity problem is the federal regulation of those who produce systems that might contain vulnerabilities. There are a variety of state statutes that regulate how companies treat customer data,[118] there are some state statutes that regulate characteristics of manufactured technology devices that influence the cybersecurity posture of their users,[119] and there are federal laws that regulate the behavior of certain industries.[120] Surprisingly, though, there is no federal regulation that specifies nationwide data security standards.[121]

The lack of federal regulation in this space may have roots in the legislature's desire not to hamstring an industry that, in the absence of heavy regulation, has become tremendously successful.[122] The light touch the United States government has applied to the Internet has resulted in a global internet where eight of the top ten most popular websites have American roots.[123] However, while applying this laissez-faire approach, the

---

[118] *See* JEFF KOSSEFF, CYBERSECURITY LAW 48–55 (Wiley, 2d ed. 2019). Chapter 1 of Jeff Kosseff's seminal work on Cybersecurity Law surveys a selection of state data security. Appendix B of the same book surveys 50 states' breach reporting statutes. *See id.* at 483–554.

[119] *See id.* at 141, 160–61 (describing California's Internet-of Things law).

[120] *See id.* at 141–67 (detailing the Gramm-Leach-Bliley Act Safeguards Rule that applies to financial institutions, the New York Department of Financial Services cybersecurity regulations, the Red Flags Rule applicable to creditors and financial institutions, the Payment Card Industry Data Security Standard self-regulation adopted by credit and debit card processors, and the much-misspelled Health Insurance Portability and Accountability Act applicable to healthcare "covered entities").

[121] *Id.* at 1.

[122] *See* 47 U.S.C. § 230 ("Actually, the federal government has removed certain regulations that apply to the rest of Americans from parts of the technology world. This approach was intended and in fact textually represents the intent to encourage the Internet to develop into "a global forum for a true diversity of political discourse."). *See also* Matthew Feeney & Will Duffield, *Six Principles for Misunderstanding Free Speech and Section 230*, CATO AT LIBERTY (Feb. 17, 2021, 11:00 AM), https://www.cato.org/blog/six-principles-misunderstanding-free-speech-section-230.

[123] J. Clement, *Most Popular Websites Worldwide as of November 2021, By Total Visits*, STATISTA (Mar. 22, 2022), https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/. Note that the URL posted in the citation is the original but has since been updated with information for 2022. The information could be located using the Wayback Machine via

technology industry's self-regulation can perhaps be measured by the prediction that cyberattacks could cost the world as much as $10.5 trillion by 2025.[124]

Despite the dire situation, it will likely be difficult for Congress to agree on how best to regulate the technology industry. For example, even within the confines of speech regulation, to say that there is not consensus regarding how to proceed is a drastic understatement.[125] It is hard to imagine that adjustments to federal cybersecurity policy would find bipartisan support given how contentious other technology policy reform conversations are in the current environment.

V. TAX EXPENDITURES AND DIRECT EXPENDITURES

To influence constituent behavior, the government can choose either to create a direct expenditure program under which payments are channeled directly to the parties in whom a behavioral change is sought or to create a tax expenditure that incentivizes behavior through the promise of lower taxes.[126] Tax expenditures represent departures from the ideal taxation policy, generally defined in terms of the Haig-Simons equation.[127] According to Stanley Surrey, such expenditures should not be considered without cost, and the methodology of direct expenditures is to be preferred.[128] However, according to Edward Zelinsky, there are distinct advantages that outweigh the inefficiencies inherent in the tax expenditure method of influencing taxpayer behavior.[129] One of those advantages is the political flexibility inherent in creating a tax expenditure as compared to

---

http://web.archive.org/web/20220322024513/https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/.

[124] Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually By 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/.

[125] *See generally* Jane Bambauer, James Rollins, & Vincent Yesue, *Platforms: The First Amendment Misfits*, 97 IND. L.J. 1047 (2022) (providing a fuller discussion of the dynamics of the debate surrounding speech regulation in the technology industry).

[126] *See* PHILIP D. OLIVER, TAX POLICY READINGS AND MATERIALS 745–802 (Thomas Reuters/Foundation Press, 3d ed. 2011).

[127] HENRY C. SIMONS, PERSONAL INCOME TAXATION 50 (The University of Chicago Press, 1965) (1938).

[128] OLIVER, *supra* note 126, at 747–54.

[129] *See* Edward A. Zelinsky, *James Madison and Public Choice at Gucci Gulch: A Procedural Defense of Tax Expenditures and Tax Institutions*, 102 YALE L.J. 1165, 1166 (1993).

the political cost associated with creating and funding a program to influence industry.[130]

The federal government makes considerable direct expenditures on cybersecurity-related projects.[131] Yet, these expenditures are siloed, coordinated only at the most general policy level, and apply largely to government contractors.[132] A different approach is needed to address systemic, nationwide problems in the private sector that affect the common interest.

Usually, a tax expenditure either boosts a new technology, giving it a toehold in the marketplace, or compensates the private sector to undertake an activity that has benefits to the commons but is not commercially practicable.[133] Here, the goal of the expenditure would be similar but not completely identical to the typical one: it would have to either compensate a technology manufacturer for foregoing the first mover advantage in favor of "building in" security before a product is launched, substituting a cash incentive for the toehold that a less-secure product could achieve via first-mover advantage; or it would incentivize the taxpayer to improve the public good by addressing the systemic security deficits caused by the entry of an insecure MVP into the market. The dynamics of the applicable tax expenditure could conceivably address one route or the other, but ideally, would incentivize both routes.

---

[130] *Id.* at 1178.

[131] OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, ANALYTICAL PERSPECTIVES, BUDGET OF THE U.S. GOVERNMENT 167 (2022).

[132] *Id.* at 165–70.

[133] Mona Hymel, *The United States' Experience with Energy-Based Tax Incentives: The Evidence Supporting Tax Incentives for Renewable Energy*, 38 LOY. U. CHI. L.J. 43, 43 n.1 (2006) (citing BRUCE W. CONE ET AL., AN ANALYSIS OF FEDERAL INCENTIVES USED TO STIMULATE ENERGY PRODUCTION 7 (1978)).

A. EXPENDITURE DESIGN

A tax expenditure designed to incentivize behavior risks failing – or worse, incentivizing the wrong behavior – if it is not carefully tailored to the desired behavior[134] For example, Corporate Average Fuel Economy (CAFE) fuel efficiency standards[135] were established with the goal of "reduc[ing] the greenhouse gas emissions and oil consumption associated with passenger transportation[.]"[136] But the version of CAFE standards in force from 2011 to 2016 did not simply mandate better fuel economy; instead, they mandate fuel economy as "a function of the footprint (wheelbase by track width) of the vehicles in a manufacturer's fleet."[137] As such, the design of the incentive drives manufacturers towards both better fuel economy and bigger vehicles, and they are left to choose which will maximize their profits.[138] To the extent that consumers are willing to pay for bigger vehicles, the CAFE standards are undermined by their design.[139] In the cybersecurity context, the optimum tax expenditure would be one focused on producers of technology products and would be one that directly incentivizes the activity that they perform to make those products more secure.

Classifying the type of influence sought by the expenditure as either increasing supply, increasing demand, or creating infrastructure often aids in selecting the form of an expenditure.[140] When an expenditure seeks to increase supply, an expenditure that provides an incentive to increase production, like an inventory credit, would be preferred.[141] An expenditure like a decrease in tax rates that puts more cash in the hands of certain consumers could drive increased demand, as could a credit or deduction associated with funds used to purchase the product in question.[142] If the goal is to spur the development of infrastructure, an expenditure consisting of accelerated depreciation for investment in that infrastructure would be

---

[134] *See generally* Kate S. Whitefoot & Steven J. Skerlos, *Design Incentives to Increase Vehicle Size Created from the U.S. Footprint-Based Fuel Economy Standards*, ENERGY POL'Y (2011).

[135] Note that CAFE standards are not tax expenditures, and that this comparison is merely for the purposes of explanation.

[136] *Id*. at 1.

[137] *Id*.

[138] *Id*.

[139] *Id*. at 9.

[140] *See generally* Roberta F. Mann & Mona L. Hymel, *Moonshine to Motorfuel: Tax Incentives for Fuel Ethanol*, 19 DUKE ENV'T L. & POL'Y F. 43 (2008).

[141] *Id.* at 47.

[142] *Id.* at 49.

preferable.[143] The correctly designed expenditure would be the one that increases the supply of secure technology products by making the development process less expensive.

Today, no expenditure exists that would directly encourage manufacturers to forego the first-mover advantage and make an up-front investment in the design of a secure architecture that would avoid the considerable technical debt inherent in creating insecure technology and then fixing it later. For logistical, political, and regulatory simplicity reasons, a modification to an increasing expenditure might be preferable to the development of a new expenditure.

The closest existing expenditure[144] is the § 41 credit for increasing research activities, which provides taxpayers with a 20 percent credit for qualified research expenses above a threshold amount.[145] This is a credit based on "amounts which are paid or incurred by the taxpayer,"[146] so to the maximum extent possible, it avoids potential gaming of the system.[147] It is a credit for performing exactly the activity desired, which serves to increase the supply of the type of product facilitated by this desired activity. Finally, the credit is an existing expenditure, which, to the maximum extent possible, avoids potential partisan political challenges, enabling an adjustment that can be made at the direction of the Executive branch.[148]

The Economic Recovery Tax Act of 1981 initially implemented the § 41 research and development credit to reverse a trend between the late 1960s and late 1970s of declining research and development expenditure of

---

[143] *Id.* at 50.

[144] I.R.C. § 174 (noting that Section 174 also allows taxpayers to amortize research and development expenses over a period of 60 months).

[145] I.R.C. § 41.

[146] *Id.*

[147] The taxpayer reaps an incentive benefit from the investment in research, but they do not reap a benefit equal to the entire amount of the investment, only a percentage. The taxpayer is responsible for the remaining costs of the investment through commercialization. Accordingly, the research and development [hereinafter "R&D"] credit is protected against abuse as compared to, for instance, a 100% research grant from the government that could be spent on any research, regardless of the possibility of successful commercialization. *See* Daniel J. Hemel & Lisa Larrimore Ouellette, *Beyond the Patents-Prizes Debate*, 92 TEX. L. REV. 303, 328 (2013).

[148] Certainly, the Executive branch cannot modify the statute, but the regulations could be modified, for example, to clarify that a new version of a software component is a new business component, not a modification of an old business component, and thus not subject to the § 41(d)(4)(A) restriction that "[a]ny research conducted after the beginning of commercial production of the business component" is not eligible for the credit. *See* § 41(d)(4)(A).

both the federally funded and privately funded modalities.[149] During this decade, such expenditures remained essentially flat in real dollars but declined as a share of gross domestic product (GDP).[150] By the time the 1981 Act was passed, U.S. "civilian" research expenditures represented 1.5% of GDP, while Japan's share was 1.9% and West Germany's was 2.3%.[151] The provision was originally scheduled to sunset after 1985, but Congress repeatedly renewed it until permanently renewing it in 2014.[152] Beginning in January of 2022, companies taking advantage of the credit must do so across five years, although both Republicans and Democrats favor removing that restriction.[153]

Although the § 41 research and development credit is the closest existing provision, a few obstacles make it impractical for use as it currently reads.

B. OBSTACLES

The current configuration of the § 41 research and development credit is such that it may not sufficiently incentivize cybersecurity investment where it would be most efficient (i.e., before commercial production) because of the significance of the first-mover advantage.[154] The current configuration also does not reach cybersecurity investment where it is most likely to occur (i.e., after commercial production) because of the narrow requirements for eligibility.[155]

Section 41(d)(4) specifies that "[a]ny research conducted after the beginning of commercial production of the business component" is ineligible for the research and development credit.[156] The same is true for

---

[149] STAFF OF JOINT COMM. ON TAXATION, 97TH CONG., GEN. EXPLANATION OF THE ECON. RECOVERY TAX ACT OF 1981 119 (Joint Comm. 1981).

[150] *Id.*

[151] *Id.*

[152] David Malakoff, *U.S. House Passes Permanent R&D Tax Credit*, SCIENCE (May 9, 2014), https://www.science.org/content/article/us-house-passes-permanent-rd-tax-credit.

[153] Laura Weiss, *Major Corporations Make Last-Ditch Push for R&D Tax Break*, ROLL CALL (Mar. 2, 2022, 10:30 AM), https://rollcall.com/2022/03/02/major-corporations-make-last-ditch-push-for-rd-tax-break/.

[154] The comparison, which is difficult to quantify, is between the 20% of the excess of qualified research expenses over the base amount, or the 14% credit for the excess above 50%, of the average qualified research expenses over the last three years versus the entirety of the advantage conferred upon the first mover into a market. *See* I.R.C. § 41(a)(1); *cf.* I.R.C. § 41(c)(4)(A).

[155] I.R.C. § 41(d)(4)(A).

[156] § 41(d)(4).

surveys and studies related to quality control.[157] The upshot of this definition is that if research and development to design secure systems happens before commercial production of a business component, it qualifies. Still, if it happens after commercial production has begun, it does not.

To understand the inconsistency between the eligibility of certain investments in technology systems for research and development and what would be needed to incentivize technology manufacturers to invest more in security, one must understand the qualitative difference between the design and manufacturing process for a physical piece of technology like an airplane as compared to that of a piece of software. Boeing's 737 aircraft and Microsoft's Windows operating system can serve as widely adopted examples of technology that have evolved to include quality improvements over a long lifespan.

The 737 product family consists of twelve different commercial models, but all are certified by the FAA under a single type certificate.[158] The number of changes made within these twelve members of the 737 family after each was launched into commercial service can be roughly tracked by examining Airworthiness Directives issued against the type, which represent "legally enforceable regulations issued by the FAA in accordance with 14 CFR part 39 to correct an unsafe condition in a product."[159] The Federal Aviation Administration has issued 661 Airworthiness Directives against the 737 between the first in 1968 and the most recent in 2022.[160] Accordingly, the 737, first flown in 1967,[161] has

---

[157] *Id.*

[158] DEPT' OF TRANSP., FAA, TYPE CERTIFICATE DATA SHEET A16WE (2023).

[159] *Airworthiness Directives*, FAA, https://www.faa.gov/regulations_policies/airworthiness_directives/ (last visited May 13, 2022).

[160] FEDERAL AVIATION ADMINISTRATION, DEP'T OF TRANSP., AIRWORTHINESS DIRECTIVES, https://www.faa.gov/regulations_policies/airworthiness_directives (last visited Nov. 24, 2023) (click on Airworthiness Directive (AD) Rules; then on the navigation stack on the left side of the page, click on Airworthiness Directives and choose the subtab entitled "AD Final Rules"; next, in the grey box, search using the following terms: In the field marked "Make," type "Boeing." From the three options that appear, select "The Boeing Company." Next to Make, there is a field for "Model." Here, type "737" and many different subtypes of 737 come up. Click the checkbox next to twelve out of the fifteen options: 737-100, 737-200, 737-200C, 737-300, 737-400, 737-500, 737-600, 737-700, 737-700C, 737-800, 737-900, and 737-900ER; from there, click "Apply" to apply the filters to the entire set of Airworthiness Directives).

[161] *Original 737 Comes Home to Celebrate 30th Anniversary*, BOEING, https://boeing.mediaroom.com/1997-05-02-Original-737-Comes-Home-to-Celebrate-30th-Anniversary (last visited November 24, 2023).

seen approximately one new version every five years and about eight and one half Airworthiness Directives per year during the fifty-six-year lifespan of the type.

Windows NT forms the basis for the Windows operating system used at the time of this writing. It has seen a great deal of incremental development since then but retains essentially the same architecture today as it did on the date of its initial commercial release in 1993.[162] Between 1993 and 2022, this line of operating systems saw approximately eleven major versions.[163] The number of changes made within these eleven versions of the Windows NT family after each was launched into commercial service can be roughly tracked by examining Microsoft's Security Updates Guide, which lists security patches issued against Microsoft products.[164] Between May 2021 and April 2022, Microsoft issued over 8,000 patches against the various subversions of Windows 10 in a single year.[165] One of the eleven major versions of Windows had almost twelve times more defects addressed in approximately twelve months than every version of 737 shipped during its nearly six-decade lifespan. Historically, Microsoft typically releases patches for its software on the second Tuesday of each month, but this practice may be changing with the launch of Windows Autopatch.[166] This change will continuously deploy hotfixes as they become available instead of waiting for a monthly deployment window.[167]

The takeaway is that the research and development model for a complex physical product and for a complex piece of software could not be more different. The example of a physical product requires certification by a government agency before commercial use, while the example of a software product requires certification for certain government use but not

---

[162] *Windows Versions*, PCMAG, https://www.pcmag.com/encyclopedia/term/windows-versions (last visited May 13, 2022).

[163] These versions include: 3.5, 3.51, 4.0, 5.0, 5.1, 6.0, 6.1, 6.2, 6.3, 6.4, and 10. *See id*; *see also* Anoop C. Nair, *Windows 11 Version Numbers Build Numbers Major Minor Build Rev*, ANOOPCNAIR.COM (Oct. 11, 2023), https://www.anoopcnair.com/windows-11-version-numbers-build-numbers-major/.

[164] *Security Update Guide*, MICROSOFT, https://msrc.microsoft.com/update-guide/ (last visited May 13, 2022).

[165] *Id.* (click "Product Family" and filter by "Windows." Select all products in the list that begin with "Windows 10").

[166] This is colloquially known as Patch Tuesday. *See* Charlie Osborne, *Microsoft's April 2022 Patch Tuesday Tackles Two Zero-Day Vulnerabilities*, ZDNET (Apr. 12, 2022), https://www.zdnet.com/article/microsoft-april-2022-patch-tuesday-two-zero-day-vulnerabilities-tackled/.

[167] *Id.*

general commercial use.[168] Improvements to the aircraft are a significant event, which might require the physical inspection of each plane suspected to contain a defect,[169] while improvements to the operating system happen almost continuously and can occur automatically.[170]

The difference in the amount of work done to maintain the quality of an aircraft versus the amount of work done to maintain the quality of an operating system after introduction to the commercial market is important from a taxation perspective. The research and development that happens after introduction to the commercial market is ineligible for the § 41 credit, while the research and development that happens before introduction is eligible. Without changes to § 41, a significant part of maintaining the quality of software over time is not incentivized by the credit.

Another obstacle is that the § 41 credit incentivizes *increases* in research and development expenditures, not steady-state expenditures.[171] In the initial formulation of the credit, twenty percent of the amounts above the historical base average were creditable.[172] Later, in an attempt to simplify the calculation for businesses, the Alternative Simplified Credit was added, wherein the creditable amount is fourteen percent above an amount equal to half of a company's average expenditures in the last three years. The result of both methods is that a rate of expenditure that is constant over a long period of time is not creditable.[173]

A third obstacle is rooted in complex accounting and record-keeping practices. Firms that seek the § 41 credit must keep a detailed accounting of research activities. It is not enough to provide the Internal Revenue Service with a list of salaries of employees involved in research or even to present a "reasonable allocation of salaries to the activities"; instead, the taxpayer must detail specific expenses associated with research

---

[168] *Certification*, FAA, (July 20, 2022), https://www.faa.gov/uas/advanced_operations/certification/; *cf. Federal Risk and Authorization Management Program (FedRAMP)*, MICROSOFT (Sept. 27, 2023), https://docs.microsoft.com/en-us/compliance/regulatory/offering-fedramp.

[169] *FAA Orders Inspection of Boeing 737 Plane Tails*, CLAIMS J. (Apr. 17, 2013), https://www.claimsjournal.com/news/national/2013/04/17/227185.htm.

[170] Liam Tung, *Microsoft: Windows Autopatch is Coming Soon. Here's What You Need to Know*, ZDNET (Apr. 7, 2022, 2:58 AM) https://www.zdnet.com/article/microsoft-windows-autopatch-is-coming-soon-heres-what-you-need-to-know/.

[171] *Tax Treatment Legislative History*, R&D COALITION, https://investinamericasfuture.org/tax-treatment-legislative-history/ (last visited May 13, 2022).

[172] *Id.*

[173] *Id.*

and development activities.[174] Under the current statute, a new firm at the stage where the credit applies (i.e., prior to the release of a new piece of software) might not be mature enough to create and maintain such records.

VI. CONCLUSION

Neither cybersecurity insurance, the development of tort law to allow strict liability for software, federal regulation, nor taxation policy reform alone will completely address America's problem with insecure technology. Modifications in all four of these areas should be deployed in a coordinated manner.

First, insurers and the government must work together to improve the effectiveness of cybersecurity insurance and mitigate its counterproductive effects. The effectiveness of cybersecurity insurance can be improved by bolstering the virtuous cycle originally envisioned by the federal government. The focus of insurance companies should be to use the leverage of lower premiums (or perhaps the very availability of insurance) to encourage insureds to change their risky behavior. The moral hazard problem presented by cybersecurity insurance and the information gap between insurer and insured will take work to conquer, but this work is critical to the security and stability of the nation. Mitigation of the counterproductive effects of cybersecurity insurance could be accomplished by a prohibition on insurance companies paying criminal extortionists, either by the insurers or, to solve the coordination problem, the government.[175] The widespread nature of this practice and the time that has passed without addressing this problem undoubtedly means there will be some short-term pain. Until this source of funding for international criminal gangs is strangled, however, the criminals will prosper, and the national security problems posed by insecure computers and networks will proliferate. One way to keep money out of the hands of criminals is to shift the burden of purchasing cybersecurity insurance away from the user, who is in a poor position to make the technology they use more secure, and toward the manufacturer, who is much better positioned to manage and spread the risk. Shifting this burden would be facilitated by the adoption of the next proposal.

---

[174] Eustace v. Comm'r, 81 T.C.M. (CCH) 1370 (T.C. 2001), 2001 WL 273672, at *6, *aff'd*, 312 F.3d 905 (7th Cir. 2002).

[175] This is perhaps less unlikely than it sounds; New York proposed such a ban in 2021. *See* Lindsey O'Donnell, *Cyber-Insurance Fuels Ransomware Payment Surge*, THREAT POST (June 1, 2021, 5:05 PM), https://threatpost.com/cyber-insurance-ransomware-payments/166580/.

Second, the law should allow for strict liability suits against software manufacturers who market insecure software. Today, such strict liability does not exist, and plaintiffs must fall back on general theories of liability. Cases like these are extraordinarily difficult to win, meaning it is difficult to apply direct leverage on those who are in the best position to ensure online safety. Making strict liability solutions available would go a long way in shifting the insurance burden from the consumer to the manufacturer.

Third, the government should create comprehensive federal legislation mandating secure products and secure practices. There are federal guidelines as to best practices; there are state-by-state data breach notification laws; there are federal laws against hacking; and there are federal agencies dedicated to understanding. On the whole, however, our legal system is totally lacking a systematic enforcement mechanism for making sure computers and networks are secure.

Fourth, the legislature should adjust the § 41 research and development credit. To defeat the perceived incentive to rush insecure MVPs to market, the amount of credit should be increased. To incentivize technology manufacturers to *sustain* research and development spending instead of *increasing* it, the credit must be reshaped to apply to all research and development spending on cybersecurity, not just a percentage of the base rate. To incentivize spending on post-commercial production cybersecurity efforts, the post-commercial production limitation for software should be removed.

These could be politically challenging measures to implement, especially when Congress seems ill-equipped to come to a bipartisan consensus around important issues related to the public good. Nevertheless, lawmakers must consider bold actions available in response to the crisis that could ensue if severe cyberattacks continue to threaten our modern, technologized way of life.