Chapman Law Review

Volume 19 | Issue 2 Article 2

2016

Moore's Law Versus "Man's" Law? How Cybersecurity and Cyber Terror Government Policies May Help or Hurt Entrepreneurial Startups

David Groshoff
American Jewish University

Moore's Law Versus "Man's" Law? How Cybersecurity and Cyber Terror Government Policies May Help or Hurt Entrepreneurial Startups

*David Groshoff**

"*Creating malware is bad, but if you sell it to police, it becomes okay. . . . We are not lawyers, we are hackers, and we know that any kind of rules can, and will, be bypassed. It is our job.*"[1]

—Raphael Vinot

INTRODUCTION

In 1965, Fairchild Semiconductor's Gordon Moore (later co-founder of Intel Corporation) indicated that "the number of transistors capable of being placed on a chip or integrated circuit quadruples every three years due to innovations and the march of technology."[2] This phenomenon has become known as "Moore's Law,"[3] with indications that Moore's Law has become exponentially faster in moving technology forward.[4]

The Internet as we know it today was essentially invented in the 1970s, and the world wide web was invented in the 1990s.[5]

---

* Chair, and Associate Professor of Business, American Jewish University, Los Angeles. Ed.M., Harvard University; J.D., The Ohio State University; M.B.A., Northern Kentucky University; B.A., Indiana University; former founding General Counsel of DreamFund.com, an infrastructure software company founded by the 2007 National Entrepreneur of the Year and three-time *Inc. 500* CEO Kent Plunkett. I thank Kent Plunkett, Yong Zhang, Peter Crosby, and Mi Tang for their assistance in understanding cybersecurity from the entrepreneur's perspective. The Article is meant to be gender-neutral, and the non-gender-neutral language in the Article's title was employed for alliteration.

1 Raphael Vinot, *On Ethics in Information Technology*, BOINGBOING (June 13, 2015, 5:00 AM), http://boingboing.net/2015/06/13/on-ethics-in-information-techn.html [http://perma.cc/ZD7G-WSP2].

2 Peter Harsha, *IT Research and Development Funding*, *in* CHASING MOORE'S LAW, INFORMATION TECHNOLOGY POLICY IN THE UNITED STATES 1, 23 (William Aspray ed., 2004); *see also* Steve Mosier, *Telecommunications and Computers: A Tale of Convergence, in* CHASING MOORE'S LAW, INFORMATION TECHNOLOGY POLICY IN THE UNITED STATES, *supra,* at 29, 37.

3 Mosier, *supra* note 2, at 37.

4 *See* Harsha, *supra* note 2, at 23; Mosier, *supra* note 2, at 37.

5 *See* Mosier, *supra* note 2, at 35–36.

Moore's Law likely applies to the Internet[6] and web as well, for good and bad, with the bad meaning that laws, rules, regulations, and policy levers cannot keep up with a rapidly moving, technology-driven economy, which has led to very recent and well-publicized cybersecurity breaches that this Symposium and this Article research and discuss.

Perhaps the most widely known cyberattack in the paradigm existing during the past several years occurred at the former Dayton-Hudson Corporation, now known as Target Corporation.[7] In this cyber breach, called a "watershed moment" in Target's hometown newspaper by at least one expert,[8] the hackers captured customer data from payment cards via malware that had unknowingly been installed in Target's computer system through a Target vendor. While the cybersecurity breach against Target occurred in 2013, affected approximately 110 million Target customers, and was the end-result of a so-called "phishing scam" from a vendor,[9] the case has already

---

6 In 1995, the Federal Network Council officially defined the Internet as:

> the global communication system that—(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

Id. at 36 (citing *Definition of "Internet,"* NETWORKING & INFO. TECH. RES. & DEV. (NITRD) PROGRAM (Oct. 24, 1995), http://www.itrd.gov/fnc/Internet_res.html [http://perma.cc/6L45-Z9ET]).

7 *See, e.g.*, *Inside Target Corp., Days after 2013 Breach*, KREBS ON SECURITY (Sept. 21, 2015, 12:01 AM), http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/ [http://perma.cc/M7DD-SAS8] (indicating that Target has since hired outside consultants). Target also has created a so-called "cyber-fusion center" to improve security and sponsored a national cybersecurity forum. *See Inside Target's Cyber Fusion Center*, A BULLSEYE VIEW (July 21, 2015), https://corporate.target.com/article/2015/07/cyber-fusion-center [http://perma.cc/5AUT-7XCL] (indicating that Target Corp. planned to invest over $1 billion in cybersecurity in 2015).

8 Tom Web, *Cyber–Security Expert: Target Case is 'Watershed Moment,'* TWINCITIES.COM (Feb. 2, 2014, 12:01 AM), http://www.twincities.com/ci_25047596/cyber-security-expert-target-case-is-watershed-moment [http://perma.cc/DB4W-8YZQ].

9 Dan Goodin, *Epic Target Hack Reportedly Began with Malware-Based Phishing E-mail: Attack Hit Contractor Two Months Before the Compromise of 40 Million Payment Cards*, ARS TECHNICA (Feb. 12, 2014, 1:00 PM), http://arstechnica.com/security/2014/02/epictarget-hack-reportedly-began-with-malware-based-phishing-e-mail/ [http://perma.cc/7H35-A7DQ]. Initially,

> 'phishing' campaigns typically involved an e-mail that appeared to be coming from [an entity] convincing users they needed to change their passwords or provide some piece of information . . . . A fake web page and users' willingness to fix the nonexistent problem led to account takeovers and fraudulent transactions.
>
> Phishing campaigns have evolved in recent years to incorporation installation of malware as the second stage of the attack.

been included in business school and management program books.[10]

This cyber breach could cost Target several billion dollars, and that is before private litigation costs.[11] Target did maintain a cybersecurity insurance policy that covered approximately $90 million, according to an S&P estimate in June 2015.[12] Further, the cyber breach caused Target executives to testify before Congress and forced the company to face federal and state investigations relative to how the cybersecurity breach occurred. In response to a Secret Service official's statement that what occurred to Target was "highly technical and sophisticated," Target's CEO, Greg Steinhafel, asserted that the statement "show[ed] [that] it's not just our operation. It would be hard for any retailer to withstand this."[13]

Despite government calls against Target in early 2014, later that year, the federal government itself announced that its Office of Personnel Management was hacked, potentially compromising the personal data of approximately 4 to 20 million existing and former federal employees.[14] U.S. officials blamed this breach on hackers from China, possibly constituting cyberespionage, as "Chinese state-sponsored hackers are the leading suspects," who relied on a method of attack known as spear phishing.[15]

VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT 12 (2015), http://www.verizonenterprise.com/DBIR/2015/. In 2013, more than two-thirds of cyber-espionage compromising incidents involved phishing. *Id.* Approximately five malware events occur every second, which is after controls including intrusion prevention systems ("IPS"), intrusion detection systems ("IDS"), firewalls, and spam filters have done their work. *Id.* at 21.

10 *See, e.g.*, ANGELO KINICKI & BRIAN K. WILLIAMS, MANAGEMENT: A PRACTICAL INTRODUCTION 37–38 (7th ed. 2016).

11 *See, e.g.*, Ashlee Kieler, *Target to Face Class-Action Lawsuit from Banks over Data Breach*, CONSUMERIST (Sept. 16, 2015), http://consumerist.com/2015/09/16/target-to-face-class-action-lawsuit-from-banks-over-data-breach/ [http://perma.cc/GCU3-RJD8].

12 *See* Sonali Basak, *Worried About a Cyber-Apocalypse? AIG Wants to Sell You a Policy*, BLOOMBERG BUSINESS (July 22, 2015, 2:00 AM), http://www.bloomberg.com/news/articles/2015-07-22/worried-about-a-cyber-apocalypse-aig-wants-to-sell-you-a-policy [http://perma.cc/D2DG-RZR6].

13 Monica Langley, *Inside Target, CEO Gregg Steinhafel Struggles to Contain Giant Cybertheft*, WALL ST. J. (Feb. 18, 2014, 10:48 PM), http://www.wsj.com/articles/SB10001424052702304703804579382941509180758.

14 *See, e.g.*, Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST (June 4, 2014), https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html [http://perma.cc/LUN2-TXBP]; *cf. infra* note 44 (referring to a twenty-million number).

15 Josh Chin, *Cyber Sleuths Track Hacker to China's Military*, WALL ST. J. (Sept. 23, 2015, 5:00 PM), http://www.wsj.com/articles/cyber-sleuths-track-hacker-to-chinas-military-1443042030. This assertion is not to suggest that the United States does not engage in cyber surveillance internally or externally. *See* Charlie Savage et al., *Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at Border*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-

Very personal websites such as Ashley Madison—the purpose of which was to assist adults in finding a partner with whom to commit adultery—were hacked in 2015. This led to the disclosure of details from 32 million accounts and the loss of human capital, in addition to financial capital, as some customers of that website committed suicide as a result of the data breach of which Ashley Madison had been forewarned.[16] The Internal Revenue Service ("IRS") admitted breaches to its system, leading to the disruption of information of approximately 300,000 people.

Simply put, cybersecurity is not a public sector issue or a private sector issue. The federal government should not be putting businesses such as Target through costly investigations while at the same time leaving the nation's power grid vulnerable, and exposing millions of people's personal information—stored by state-sponsored government entities such as UCLA's medical system and the IRS—to data breaches.[17] Even software technology companies have been hacked in the past year, as Apple, Inc. became victim in mid-September 2015.[18] To attempt to combat the various forms of cyber-rattling that have been occurring, a number of discussions have taken place offering a variety of proposals, including this Symposium.

However, one hugely important sector of the U.S. economy that appears to be ignored in all of this discussion is the plight of risk management relative to cybersecurity for the entrepreneur. For purposes of this Article, "entrepreneur" means a startup enterprise or the founder of a startup entity for which the end-goal is that the entity scale to the point of an initial public offering ("IPO") under U.S. securities regulations or an acquisition of the business. This Article considers the risks and costs and policy arguments relative to attempting to run a lean—non-cybersecurity—startup, while simultaneously attempting to disrupt industries and compete with existing rivals in the public, private, and government sectors that have proven

---

spying-at-us-border.html [http://perma.cc/4LQC-FZNL].

16 *See, e.g.*, Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN MONEY (Sept. 8, 2015, 7:10 PM), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/index.html [http://perma.cc/CVC4-5QAA]; *see also* Chris Isidore & David Goldman, *Ashley Madison Hackers Post Millions of Customer Names*, CNN MONEY (Aug. 18, 2015, 12:39 AM), http://money.cnn.com/2015/08/18/technology/ashley-madison-data-dump/index.html?iid=EL [http://perma.cc/2ZCZ-VAYM] (stating that a month prior to the data release, the hackers, calling themselves the "Impact Team," indicated they would hack and release the information obtained unless the website ceased operations).

17 *IRS Breach Bigger than Thought*, CNBC (Aug. 17, 2015, 2:07 PM), http://video.cnbc.com/gallery/?video=3000407838.

18 Yang Jie & Josh Chin, *Apple iOS Breach No Mere 'Mistaken Experiment,' Chinese Experts Say*, WALL ST. J.: CHINA REAL TIME (Sept. 21, 2015, 8:55 PM), http://blogs.wsj.com/chinarealtime/2015/09/21/prank-or-hack-apple-china-breach-in-eye-of-beholder/.

incapable of protecting themselves or their respective customer bases, despite employing costly protective measures.

The Article first briefly provides an historical framework—including contextualizing recent events—regarding cybersecurity. Next, the Article discusses what options are available to businesses, due to the many recent breaches and failures of government to defend against cyber hacking and cyber terror, and then bifurcates the options available to established businesses and startup entrepreneurial businesses. Third, the Article discusses existing material cyberlaws, regulations, and executive orders, as well as laws proposed by President Obama in early 2015. Fourth, the Article uses those existing and proposed rules to examine the pros and cons of applying a public-private partnership to combat cyberthreats versus employing a purely market-based solution.

Finally, the Article argues, and underpins with policy proscriptions, that due to the huge differences between established businesses and entrepreneurial startups, their legal responsibilities should be placed under the rubric of a sliding scale of fiduciary duties of care relative to personally identifiable information ("PII") and cyberattack mitigation, based on a business's size, scale, and duration since formation. This Part also proposes that each state mandate corporations, limited liability companies, and other owner liability-shielded entities require a risk management committee of its board of directors or governing body. The Article concludes that, due to the many moving parts that exist in this area, the private sector should lead the way in cyber protection, including self-policing and certifying. Solely foreign governmental attacks on domestic U.S. private or governmental cyber-hacking entities require a federal mandate on businesses, rather than cyber hackers, that impact U.S. citizens, businesses, and financial capital.

I. BACKGROUND ON CYBERSECURITY AND CYBER LAW

A. Lack of Meaningful Historical Guidance

Given that the majority of examples of cyber-hacking described in this Article's introduction occurred after the *Chapman Law Review*'s announcement of this Symposium, one can reasonably understand how quickly the field of cybersecurity is moving relative to other areas of law and policy. For example, the initial federal statute concerning computer crimes occurred

in 1984.[19] Less than three years old, 2013's *Internet and Online Law*,[20] a practice guide, already seems dated relative to its awareness or discussion of the existing and looming cybersecurity threat. Although that text contains a robust section entitled "Privacy, Data Protection and Related Issues,"[21] none of the numerous statutes, regulations, rules, and common laws mentioned in the text are able to prevent any material cybersecurity matters or materially affect a business' cybersecurity attempts.

Another text, *Technology Innovation Law and Practice Cases and Materials*,[22] while again providing robust discussion on other areas of law and technology, is essentially silent on cybersecurity and cybercrime.[23] Subsequent cases have been largely ineffective to prevent or deter cybercrime.[24] Worse, during several cybercrimes

---

19 Act of Oct. 12, 1984, Pub. L. No. 98–473, § 2102(a), 98 Stat. 1837, 2190 (codified as amended at 18 U.S.C. 1030 (2012)); *see also* United States v. Morris, 928 F.2d 504, 507 (2d Cir. 1991).

20 KENT D. STUCKEY, INTERNET AND ONLINE LAW (2013); *cf.* CLIFFORD ENNICO, ADVISING EBUSINESSES §§ 11:1–11:15 (2011–2012 ed.) (stating essentially same).

21 *See* STUCKEY, *supra* note 20, §§ 5.01–5.03 (describing the many acts affecting privacy rights online including: (a) the Mail Privacy Statute; (b) Electronic Communications Privacy Act and Stored Communications Act; (c) the Communications Assistance for Law Enforcement Act, Computer Fraud and Abuse Act; (d) Federal Trade Commission Act; (e) Children's Online Privacy Protection Act ("COPPA"); (f) USA Patriot Act; (g) Health Insurance Portability and Accountability Act ("HIPPA"); (h) Graham-Leach-Bliley Act; (i) Common Law Invasion of Privacy Torts; (j) Fair Credit Reporting Act; (k) Fair and Accurate Credit Transactions Act; (k) State Laws and Requirements Imposed on States by the Federal Government; (l) the Stored Communications Provisions of the Electronic Communications Privacy Act; and (m) general descriptions of consumer privacy, identity theft, and the "tension" between public and "hyper-public" information).

22 THEODORE M. HAGELIN, TECHNOLOGY INNOVATION LAW AND PRACTICE CASES AND MATERIALS (2011).

23 *See id.*

24 *See, e.g.*, United States v. Nosal, 676 F.3d 854, 859–60 (9th Cir. 2012) (interpreting the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and stating that "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved"). *But cf.* United States v. John, 597 F.3d 263, 270–73 (5th Cir. 2010) (stating that employees may exceed permissible use of employer data of customer information); United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010) (holding that a government employee of the Social Security Administration exceeded permissible access under the law when obtaining personally identifiable information regarding romantic and former romantic interests of the government employee); People v. Harris, 945 N.Y.S.2d 505, 511–13 (Crim. Ct. 2012) (using the Stored Communications Act to quash a subpoena to obtain information regarding a Twitter account and worrying that an overbroad interpretation of the Stored Communications Act would lead to "litigation by hypothetical," which "becomes particularly risky in the face of ever-evolving and ever-more-complicated technology"). Regardless, the penalties against the wrongdoers under this regulatory scheme do little to protect personally identifiable information, consumers, and customers in any material way, and as this Article's introduction suggested, these cases, even when a violation may exist, appear to do little to dissuade large-scale cybercrime.

or related criminal cases, jurors have inappropriately used social media in contravention of court orders or rules.[25]

Further, according to Verizon's 2015 *Data Breach Investigations Report*, the *New York Times* employed the term "data breach" in 700 articles in the year 2014, up from fewer than 125 articles just one year earlier.[26] Additionally, Verizon reported that 2014 became the year that the data breach was of the "cyber" variety.[27] Moreover, these articles described nearly 80,000 cybersecurity incidents, with more than 2000 confirmed breaches, affecting 700 million compromised records and costing $400 million in financial losses in 2014.[28] While the top three affected industries in 2014 were the same as in previous years of Verizon's studies since 2008—Public, Information, and Financial Services—Section C of this Part describes a broader set of industries that have become increasingly relevant during 2015,[29] because of (1) Moore's Law, (2) Verizon's conclusion that mobile app problems were not a problem as of year-end 2014,[30] and (3) although "anything that leads to the discovery of an incident is worthwhile . . . in most cases, context is key."[31]

B. Paucity of Case Law and Academic Writing on the Matter

In conducting initial research for this Article in the late Spring of 2015, I conducted a Lexis database search using the term "cybersecurity" and located only ninety-five cases—underscoring the current importance of the case law cited earlier[32]—and fewer than two dozen relevant law journal articles.[33] I believe it is safe for me to assert at this time that technology and human action in this arena are well ahead of meaningful protective legal and policy instruments. For a current example—albeit in a slightly different arena of business disruption—that illustrates technology outpacing the extant legal regime, one need simply review Uber's and Lyft's business models versus traditional taxi cabs.[34]

---

25 *See, e.g.*, United States v. Fumo, 655 F.3d 288, 298 (3d Cir. 2011); Commonwealth v. Werner, 967 N.E.2d 159, 167–69 (Mass. App. Ct. 2012).

26 VERIZON, *supra* note 9, at 1.

27 *Id.*

28 *Id.*

29 *Id.* at 3.

30 *Id.* at 18–19 (stating that FireEye, Inc.—discussed *infra* note 89 and accompanying text—indicated that under 0.03% of smartphones per week had malicious code infections based on 1400 EnPublic Apps, and Kindsight Security Labs' biannual report indicated a rate of 0.68%); *see also Motive Security Labs Malware Reports*, ALCATEL LUCENT, www.alcatel-lucent.com/solutions/malware-reports [http://perma.cc/7B5M-NDFP].

31 VERIZON, *supra* note 9, at 11.

32 *See supra* notes 19, 24–25 and accompanying text.

33 Screen capture on file with author.

34 *See, e.g.*, Andrei Hagiu, *Work 3.0: Redefining Jobs and Companies in the Uber Age*, HARV. BUS. SCH. (Sept. 29, 2015), http://hbswk.hbs.edu/item/work-3-0-redefining-jobs-and-

C. Industry Examples of Real Consequences Beyond the Consumer Phase

1. Recent Concurring Black Swan Events Across Industries

During 2015, society witnessed black swan cybersecurity events, such as simultaneous cyber outages to major components of U.S. industry. For example, first, on July 8, 2015, at approximately 10:00 a.m., one of the nation's largest airlines, UAL/Continental grounded its flights due to cyber problems, with the company's former CEO describing UAL as "100% dependent on IT."[35] Second, at approximately 11:32 a.m. on the same day, the New York Stock Exchange's ("NYSE's") computer infrastructure failed, leading to the longest suspension of trading (and the cancelling of all prior trades) since at least the so-called "flash-crash" of 2009.[36] Third, during this time on the same day, the financial media websites of the *Wall Street Journal* and *ZeroHedge* also failed.[37]

The confluence of these events led not only to spikes in the share prices of cybersecurity firms once share trading resumed,[38] but also to two Justice Department officials commenting on the matter, President Obama being briefed on the issue and subsequently issuing a statement, the involvement of the Federal Bureau of Investigation ("FBI"), and a statement from the Department of Homeland Security ("DHS").[39] Eerily, on the eve

---

companies-in-the-uber-age [http://perma.cc/3YMX-5DHU].

35 *UAL 100% Dependent on IT: Former Continental CEO,* CNBC (July 8, 2015, 10:11 AM), http://video.cnbc.com/gallery/?video=3000395071; *United Flights Grounded Due to Computer Issue*, CNBC (July 8, 2015, 9:51 AM), http://video.cnbc.com/gallery/?video=3000395056.

36 *UAL 100% Dependent on IT: Former Continental CEO*, *supra* note 35; *United Flights Grounded Due to Computer Issue*, *supra* note 35.

37 *See*, *e.g.*, Tyler Durden, *And Now the Wall Street Journal Is Down*, ZEROHEDGE (July 8, 2015, 11:50 AM), http://www.zerohedge.com/news/2015-07-08/wall-street-journal-down [http://perma.cc/3RU3-6XJB]; *see also* Kaja Whitehouse, *WSJ, Barrons Hacked: CEO Warns of Wider Plot*, USA TODAY (Oct. 9, 2015, 5:06 PM), http://www.usatoday.com/story/money/2015/10/09/barrons-hacked-ceo-warns-wider-plot/73663568/ [http://perma.cc/3KJB-REWG] (indicating that the *Wall Street Journal* announced in October 2015 that the business has been hacked multiple times since at least 2012).

38 *See, e.g.*, *FactorShares Trust PureFunds ISE Cyber Security ETF*, MARKETWATCH (July 8, 2015), http://www.marketwatch.com/investing/fund/HACK/historical?siteid=mktw&date=July%208%2C%202015&userName=&password=&remChk=on&returnUrl=&persist=&x=15&y=12 [http://perma.cc/K4JM-VV46] (rising more than 1.7% for a basket of cybersecurity stocks on more than double the average daily trading volume for the stock); *see also CyberArk Software Ltd.,* MARKETWATCH (July 8, 2015), http://www.marketwatch.com/investing/stock/CYBR/historical?siteid=mktw&date=July%208%2C%202015&userName=&password=&remChk=on&returnUrl=&persist=&x=0&y=0 [http://perma.cc/7ASB-HKUT] (rising more than 8.8% in intra-day trading for cybersecurity firm CyberArk discussed *infra*).

39 *See, e.g.*, *FBI: Monitoring Situation at NYSE*, CNBC (July 8, 2015, 12:39 PM), http://video.cnbc.com/gallery/?video=3000395115; *Homeland Security: No Nefarious Actor*

of this non-harmonic convergence, a mysterious tweet predicted the occurrence of the highly improbable event of the NYSE's shutdown.[40]

However, a meaningful question remains as to how much of a black swan event this instance in July 2015 was.[41] Only a month earlier, in June 2015, former FBI agent Austin Berglas—who in 2009 created the New York branch of the FBI's cybercrime unit—described a hypothetical scenario in which the NASDAQ market, the New York subway system, and Con Edison (New York City's largest gas and electric company) all simultaneously went offline.[42] Con Edison is part of the public-private U.S. power grid, which, according to representatives of the federal government, contains vulnerabilities that could cost approximately $1 trillion to secure.[43]

2. Public Sector: U.S. Government, Cybersecurity, and Cyberterrorism

Moving from the private to the public sector, as discussed earlier in this Article, the U.S. government was subjected to a material cybersecurity breach in late 2014. The size and scope of this breach are still unknown, but it is believed to have affected approximately 20 million people in the United States,[44] and the

---

in United and NYSE Issues, CNBC (July 8, 2015, 1:25 PM), http://video.cnbc.com/gallery/?video=3000395165; *No Indications United and NYSE Glitches Related*, CNBC (July 8, 2015, 12:02 PM), http://video.cnbc.com/gallery/?video=3000395110; *White House: President Briefed on NYSE Halt*, CNBC (July 8, 2015, 1:36 PM), http://video.cnbc.com/gallery/?video=3000395167.

40 *See, e.g.*, Jesse Byrnes, *Anonymous Issued Cryptic Tweet on Eve of NYSE Suspension*, HILL (July 8, 2015, 1:55 PM), http://thehill.com/policy/finance/247225-anonymous-issued-cryptic-tweet-on-eve-of-nyse-suspension [http://perma.cc/6XXR-V4NJ]. For more information regarding the group known as "Anonymous," see *infra* note 70.

41 *See, e.g.*, Edward Helmore, *The New Sage of Wall Street*, GUARDIAN (Sept. 27, 2008, 7:01 PM), http://www.theguardian.com/books/2008/sep/28/businessandfinance.philosophy [http://perma.cc/4AMW-EHC5] ("['Black swan event'] refers to the medieval belief that all swans were white, hence black swan was a metaphor for something that could not exist, a metaphor that shifted into a perceived impossibility that came to pass when black swans were discovered in the 17th century."). *See generally* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2010); Bill Conerly, *Uncertainty and Risk Management: What to Do About Black Swans?*, FORBES (Feb. 20, 2013, 5:34 PM), http://www.forbes.com/sites/billconerly/2013/02/20/uncertainty-and-risk-management-what-to-do-about-black-swans/.

42 Basak, *supra* note12.

43 *See Protecting US Power Grid from Hack Attack*, CNBC (June 30, 2015, 8:43 AM), http://video.cnbc.com/gallery/?video=3000392902 (showing Elizabeth Sherwood-Randall, Deputy Secretary of Energy, discussing federal attempts to protect the nation's power from cybersecurity threats); *see also* Ben DiPietro, *Attack on U.S. Electrical Grid Could Cost $1 Trillion*, WALL ST. J. (July 8, 2015, 10:44 AM), http://blogs.wsj.com/riskandcompliance/2015/07/08/attack-on-u-s-electrical-grid-could-cost-1-trillion/.

44 *See, e.g.*, Matt Spetalnick & Michael Martina, *Obama Announces 'Understanding' with China's Xi on Cyber Theft but Remains Wary*, REUTERS (Sept. 26, 2015, 8:19 AM), http://www.reuters.com/article/2015/09/26/us-usa-china-idUSKCN0RO2HQ20150926

IRS cybersecurity breach is apparently larger than first thought,[45] including the government workers mentioned earlier in this Article. Further, when Chinese President Xi Jinping visited the United States in September 2015, cybersecurity threats—arguably cyberterrorism—became a meaningful topic of discussion between Jinping and President Barack Obama.[46]

3. Technology Sector: Apps and Snapchat

Even the software industry can get hacked. In September 2015, Apple's iOS app store was hacked by malware.[47] A code named XCodeGhost—rather than the intended-to-be-used-code called XCode—fooled app developers into injecting malware-infected code into the apps they were creating.[48] This malware could steal users' logins or send false prompts. Apple did not indicate how many apps or users were affected by that cyber breach.[49] Many of the infected apps were located in the China app store.[50]

Through 2014, Symantec has identified more than 1 million apps "that are classified as malware,"[51] including crypto-ransomware.[52]

Another technology company to suffer a cyberhack includes the popular picture posting platform, Snapchat.[53]

[http://perma.cc/K2SK-KF5S] (suggesting that government-to-government cyberspying "could include the massive hack of the federal government's personnel office this year that compromised the data of more than 20 million people"); *see also* Jackie Northam, *Obama Meets with China's President Amid 'Enormous Strain' Between Nations*, NPR (Sept. 24, 2015, 7:35 AM) http://www.npr.org/2015/09/24/443053658/obama-meets-with-chinas-president-amid-enormous-strain-between-nations [http://perma.cc/5KL2-NWLL] ("[T]his two-day visit by President Xi Jinping comes during a particularly turbulent time in U.S.-China relations.").

45 *See, e.g.*, *IRS Breach Bigger than Thought*, CNBC (Aug. 17, 2015, 2:07 PM), http://video.cnbc.com/gallery/?video=3000407838 (estimating over 330,000 taxpayers having their PII breached from the IRS).

46 *See, e.g.*, Spetalnick & Martina, *supra* note 44 (indicating, inter alia, the discussion occurred amid "growing U.S. complaints about Chinese hacking of government and corporate databases, and the suspicion in Washington that Beijing is sometimes behind it").

47 Josh Chin, *Malware Creeps into Apple Apps*, WALL ST. J., Sept. 21, 2015, at B1.

48 *Hack Attack on Apple's iOS App Store*, CNBC (Sept. 21, 2015, 9:00 AM), http://video.cnbc.com/gallery/?video=3000422910.

49 *Id.*

50 *Id. But see generally Anti-theft Protection for iOS (Apple) Wireless Handsets*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-for-ios-apple-wireless-handsets [http://perma.cc/6HMT-A5KU] (last updated June 2015) (representing, respectively, app and cyber protection apps for mobile devices); KNOW MY APP, http://www.knowmyapp.org/ [http://perma.cc/8H3C-7GHH].

51 SYMANTEC, INTERNET SECURITY THREAT REPORT 19 (Apr. 2015) https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf [http://perma.cc/6EXV-KEQE].

52 *Id.* at 25.

53 *See, e.g.*, Byron Tau & Elizabeth Dwoskin, *White House Proposes Consumer*

4. Non-profit and Medical Sector: UCLA Health

UCLA Health, a well-known health services provider that has a number of famous celebrities among its client base due to its geographic location, was breached in the summer of 2015, impacting the PII and medical records of approximately 4.5 million patients.[54] Reviewing cybersecurity in the medical sector, from a legal perspective, some cyber-risk management firms, such as Kroll, described later in Part II, have been able to work with legal counsel to demonstrate to government attorneys that the manner in which data had been saved by the hospital was equivalent to encryption, so the state's attorney general recognized the matter as an exception to state law.[55]

Despite being highly regulated by government administrative agencies, data breaches in the healthcare industry often involve matters of life and death. For example, Gartner, Inc., a technology-research company whose ticker symbol on the NYSE is "IT" (i.e., "information technology"), indicated at the 2015 ITxpo that the Food and Drug Administration ("FDA") recently recommended the removal from commerce of an insulin pump due to the potential of the pump being hackable in hospital networks.[56] Symantec indicated that in addition to insulin pumps, pacemakers also are at risk.[57]

5. The Connected Car: Automobile Sector Cyber Hacking

Cybersecurity issues in the automotive industry can also involve life-and-death situations.[58] In July 2015, "two veteran cybersecurity researchers . . . used a software vulnerability . . . to break into a Jeep Cherokee being driven on the highway, intensifying the debate about the safety of increasingly connected cars and trucks."[59] The Jeep cyberhack affected air conditioning,

---

Cybersecurity Measures, WALL ST. J. (Jan. 12, 2015, 2:08 PM), http://www.wsj.com/articles/white-house-to-propose-consumer-cybersecurity-measures-1421068868.

54 *See, e.g.*, Chad Terhune, *UCLA Health System Data Breach Affects 4.5 Million Patients*, L.A. TIMES (July 17, 2015, 5:51 PM), http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html [http://perma.cc/RX69-XTVS]. For information regarding the predictable class action lawsuit that followed, see Ortiz v. UCLA Health System, No. BC589327 (Cal. Super. Ct. L.A. Cty. July 29, 2015).

55 *Risk Analysis – University Medical Center*, KROLL, http://www.kroll.com/en-us/intelligence-center/case-studies/cyber-security/risk-analysis-university-medical-center [http://perma.cc/23DC-BT57].

56 Tom Loftus, *Cybersecurity Becomes Life or Death Issue as Companies Add Tech to Consumer Devices*, WALL ST. J. (Oct. 6, 2015, 8:08 PM), http://blogs.wsj.com/cio/2015/10/06/cybersecurity-becomes-life-or-death-issue-as-companies-add-tech-to-consumer-devices/.

57 SYMANTEC, *supra* note 51, at 29.

58 I acknowledge that this Section's title could have referred to the "Internet of Things," rather than the automobile industry. The "Internet of Things" refers to "embedded computing devices with Internet connectivity." *Id.* at 26.

59 Abhirup Roy, *Harman Says Car Hacking Risk Restricted to Fiat Chrysler*,

windshield wipers, and "cut the transmission," leading the car's accelerator to immediately stop functioning.[60]

And in August 2015, researchers at the University of California, San Diego indicated that they successfully cyberhacked a 2013 Chevrolet Corvette.[61] This breach apparently permitted the researchers to send messages to the vehicle that not only operated windshield wipers but also tampered with brakes while the vehicle was driving.[62] As a result, these cyberhacks in the auto space evidence that the accelerators and brakes, among other devices, in automobiles are vulnerable to cybercrime that could have fatal consequences. A recent article posed the question regarding cybersecurity and connected cars, inquiring whether an industry-generated solution "without any [g]overnmental approval is the right strategy."[63]

6. Policy Tensions: Privacy Concerns Versus Cyberterrorism Protection Efforts

Further questioning government-involved solutions is the testimony in June 2015 of a FBI official before Congress indicating that the FBI faced a challenge to "[work] with tech companies 'to build technological solutions to prevent encryption above all else.'"[64] Simply put, this means that the FBI wanted the government to "make tech companies build in ways for law enforcement to access secured content from their products."[65] The FBI official, Michael B. Steinbach, assistant director of the FBI's Counterterrorism Division, also oddly disputed the "back door"

REUTERS (Aug. 4, 2015, 4:32 PM), http://www.reuters.com/article/us-fiat-chrysler-hacking-harman-intl-ind-idUSKCN0Q91TV20150804 [http://perma.cc/7KAF-5TAF]; *see also* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—with Me in It*, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [http://perma.cc/ZA3D-ZEB3] (recounting the experience of being in a moving car that gets remotely hacked).

60 Greenberg, *supra* note 59.

61 Andy Greenberg, *Hackers Cut a Corvette's Brakes via a Common Car Gadget*, WIRED (Aug. 11, 2015, 7:00 AM), http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/ [http://perma.cc/5WY6-P7LF]; *see also* Pete Bigelow, *Chevy Corvette Is Latest Car Breached by Hackers*, AUTOBLOG (Aug. 11, 2015, 7:20 PM), http://www.autoblog.com/2015/08/11/chevy-corvette-car-hackers/ [http://perma.cc/W43E-ARPK]; Mrlanrat, *Fast and Vulnerable*, YOUTUBE (Aug. 11, 2015), https://www.youtube.com/watch?v=-CH9BvFlrGs (employing a video demonstrating this type of cyberhack of automobiles).

62 Bigelow, *supra* note 61.

63 Giulio Coraggio, *Car Makers Join Forces for Connected Car Cyber Security*, TECHNOLOGY'S LEGAL EDGE (Aug. 27, 2015), http://www.technologyslegaledge.com/2015/08/27/car-makers-join-forces-for-connected-car-cyber-security/ [http://perma.cc/A48D-LK58].

64 Andrea Peterson, *FBI Official: Companies Should Help Us 'Prevent Encryption Above All Else*,*'* WASH. POST (June 4, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/04/fbi-official-companies-should-help-us-prevent-encryption-above-all-else/ [http://perma.cc/5SCL-ECR8].

65 *Id.*

that software engineers and coders use as access points to enter otherwise secure software.[66]

But this FBI proposal arguably weakens cybersecurity[67] because, for example, hackers could use the same back door as the government, and the proposal conflicts with some existing state law.[68] Further, from a policy perspective, the proposal puts legitimate privacy rights concerns at loggerheads with the legitimate national security concerns described in this Part. Moreover, as the CEO of Axeon, Inc., a company offering cyber insurance, stated: "[N]o CISO wants to create a vulnerability for him or herself by giving out the combination to the back door."[69] Another problem related to the government potentially acting overzealously in its prosecution of cyberhacks is described in the next sub-section.

7. Government and Third-Party Overreaching Responses to a Cybersecurity Breach

The government's and the Massachusetts Institute of Technology's ("MIT's") response to—and arguable cause of—the suicide of twenty-six-year-old hacker Aaron Swartz, appears disappointing.[70] Swartz successfully hacked into MIT's electronic JSTOR academic database to make innocuous academic information publicly available—actions seemingly fitting within MIT's own stated goals for "open education" and support for "hackathons."[71] Yet, despite those goals, Swartz was relentlessly pursued by MIT and government authorities, to the tune of thirteen felony counts and at least fifty years in prison.[72] These acts by government attorneys and MIT ostensibly led Swartz to

---

66 *Id.*

67 *Id.*

68 *See, e.g.*, COMMONWEALTH OF MASS. OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, A SMALL BUS. GUIDE: FORMULATING A COMPREHENSIVE WRITTEN INFO. SEC. PROGRAM, http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf [http://perma.cc/82KV-LL7E].

69 Christopher P. Skroupa, *The Insurance Industry's Vantage Point on Cyber Security*, FORBES (July 9, 2015, 5:42 PM), http://www.forbes.com/sites/christopherskroupa/2015/07/09/the-insurance-industrys-unique-vantage-point-on-cyber-security/#530e2a1a7f9d (CISO stands for Chief Information Security Officer).

70 Sam Gustin, *Aaron Swartz's Suicide Prompts MIT Soul-Searching*, TIME (Jan. 14, 2013), http://business.time.com/2013/01/14/mit-orders-review-of-aaron-swartz-suicide-as-soul-searching-begins/ [http://perma.cc/NPN9-U9F6]; *see also* Lawrence Lessig, *Why They Mattered: Aaron Swartz*, POLITICO (Dec. 22, 2013), http://www.politico.com/magazine/story/2013/12/aaron-swartz-obituary-101418 [http://perma.cc/X8NJ-CUTB].

71 *Hackathon,* RECLAIM OPEN LEARNING, http://open.media.mit.edu/hackathon/ [http://perma.cc/VV7K-9HEF].

72 Tim Cushing, *US Government Ups Felony Count in JSTOR/Aaron Swartz Case from Four to Thirteen*, TECHDIRT (Sept. 18, 2012, 7:42 AM), https://www.techdirt.com/articles/20120917/17393320412/us-government-ups-felony-count-jstoraaron-swartz-case-four-to-thirteen.shtml [http://perma.cc/4NQB-Q4M4].

the point where Swartz believed that he could no longer live his life. MIT's appalling behavior regarding this cybersecurity matter is telling, not only because the school prides itself on its tradition of hacking and its alleged desire of "open learning,"[73] but also because, according to tenured Harvard Law Professor and law and technology expert, Lawrence Lessig, a friend of the young Swartz, JSTOR declined to pursue any action against Swartz and requested that the government drop its case against Swartz.[74]

Swartz's suicide led to MIT being hacked again by so-called "hacktivists" known only as "Anonymous,"[75] who are discussed later in this Article.[76] I hope that Swartz's hacking legacy remains an important part of big data and cybersecurity discussions, particularly because he came from a university famous for "hacking." However, none of the charges brought against Swartz would have prevented or stopped the events described in this Article. Yet, what I am not observing in the legal, business, or financial media is a rational discussion of the real economic carnage—not the made-up kind that Professor Lessig alleged occurred with Swartz[77]—that can occur from a cybersecurity breach.

8. 401(k)s and Other Defined Contribution Plans, Investment, and Savings Accounts

I accept that, frankly, the loss of some of my customer or personally identifiable information in a data breach that occurs at a retailer such as Target, is not hugely impactful to me. For well over a decade, anyone could go online and purchase my

---

73 *See generally HackMIT 2015,* HACKMIT, https://hackmit.org/ [http://perma.cc/RKW8-655C] (discussing MIT's largest Hackathon); MIT HACKING MEDICINE, http://hackingmedicine.mit.edu/ [http://perma.cc/BC6C-X8C2] (stating "[w]hy we should all hack medicine").

74 *See* Gustin, *supra* note 70; Lawrence Lessig, *Prosecutor as Bully*, LESSIG BLOG V2, http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully [http://perma.cc/GQ6C-ABUT]; Juan Carlos Perez, *Hactivist, Internet Innovator Aaron Swartz Commits Suicide,* PCWORLD (Jan. 12, 2013, 4:47 PM), http://www.pcworld.com/article/2025165/hactivist-internet-innovator-aaron-swartz-commits-suicide.html [http://perma.cc/Z7AP-LJ7T] (indicating Professor Lessig's friendship with Swartz).

75 For more regarding the group Anonymous and hacking, see Gustin, *supra* note 70 and accompanying text.

76 *Anonymous Hactivists Target MIT's Websites over Aaron Swartz Suicide*, TELEGRAPH (Jan. 14, 2013, 11:45 AM), http://www.telegraph.co.uk/technology/news/9800257/Anonymous-hacktivists-target-MIT-websites-over-Aaron-Swartz-suicide.html [http://perma.cc/RNT2-493Q].

77 *See* Lessig, *supra* note 74 ("[A]nyone who says that there is money to be made in a stash of ***ACADEMIC ARTICLES*** is either an idiot or a liar. It was clear what this was not, yet our government continued to push as if it had caught the 9/11 terrorists red-handed. Aaron had literally done nothing in his life 'to make money.'") (emphasis in original).

social security number, residential address, telephone information, and the like. I recognize that my financial liability for unauthorized charges to my credit cards is fifty dollars. An inconvenience, yes, but putting me on the verge of bankruptcy, no. But an example of what may put people on the verge of bankruptcy—or being forced to eat cat food in retirement—occurred in October 2015, as Scottrade, a well-known discount securities broker was hacked.[78] Seemingly, only a matter of time exists before one of the major 401(k) custodians or providers is hacked, which could lead to unauthorized trading or funds disappearing from accounts.

Despite 2014 data indicating that the financial services sector permitted the least amount of malware events per week (an average of 350 per week),[79] in 2014, the largest of the "too big to fail"[80] banks, JPMorganChase & Co.,[81] faced a cyber breach that impacted over 70 million customers. Even if one believes that a life savings stuffed in an account insured by a federal agency, the Federal Deposit Insurance Corporation ("FDIC"), is safe, FDIC insurance applies to bank failures, not necessarily cyberattacks, unless those attacks ultimately lead to a bank failure in which the bank is placed in receivership by the FDIC.[82] Therefore, the retirement and financial security of persons in the United States is vulnerable to a myriad of unknown cyberthreats, with unknown financial consequences, because of unknown, unwritten, or outdated policies that are essentially impossible to keep up with the rapid pace of technological advancement as described by Moore's Law. Simply because trades were reversed on the day of the NYSE's ostensible software failure in July 2015, does not mean that the same result would occur following the next cyber terror attack on the NYSE or on a different securities market.

---

78 Jacob Pramuk, *Scottrade Data Breach Affects up to 4M Customers*," CNBC (Oct. 2, 2015, 2:57 PM), http://www.cnbc.com/2015/10/02/Scottrade-data-breach-affects-up-to-4m-customers.html [http://perma.cc/PR38-QKX3].

79 VERIZON, *supra* note 9, at 21.

80 *See* David C. Wheelock, *Too Big to Fail: The Pros and Cons of Breaking up Big Banks,* REGIONAL ECONOMIST 10 (Oct. 2012), https://www.stlouisfed.org/~/media/Files/PDFs/publications/pub_assets/pdf/re/2012/d/Too_Big_To_Fail.pdf [http://perma.cc/RD95-XN3F] (indicating that JPMorgan Chase was the largest of the big banks); *see also* Halah Touryalai, *The World's 29 Too Big to Fail Banks, JPMorgan at the Top*, FORBES (Nov. 11, 2013, 4:27 PM), http://www.forbes.com/sites/halahtouryalai/2013/11/11/the-worlds-29-too-big-to-fail-banks-jpmorgan-at-the-top/.

81 For the purposes of full disclosure and disclosing any potential conflicts of interest, I was a JPMorganChase & Co. officer for more than a decade, and the entity is an unsecured creditor of mine on a currently undrawn account.

82 *See, e.g.*, FED. DEPOSIT INS. CORP., YOUR INSURED DEPOSITS (2014), https://www.fdic.gov/deposit/deposits/brochures/Your%20Insured%20Deposits%20-%20English.pdf [http://perma.cc/AFG3-SJ2W]; *see also* Federal Deposit Insurance Act of 1950, Pub. L. No. 81-797, 64 Stat. 873 (codified as amended at 12 U.S.C. § 1811 (2012)).

II. WHAT DO THE ESTABLISHED PRIVATE SECTOR AND GOVERNMENTAL FAILURES TO ADEQUATELY DEFEND AGAINST CYBERCRIME AT THIS NASCENT STAGE MEAN FOR THE ENTREPRENEUR?

This Article has so far demonstrated that, to date, the public and private sectors have not thwarted material cyberattacks against the United States and its established businesses. Yet, e-commerce sales represented more than $3 trillion in 2013,[83] and according to consulting firm McKinsey, from 2004–2009, electronic transactions represented 15% of U.S. gross domestic product ("GDP") growth.[84] To understand what cybersecurity means for the entrepreneurial startup enterprise, however, one must first understand the milieu in which larger, traditional, or established businesses operate in their attempts to manage the risk of cyberattacks. This Part begins by looking at data points of what those established business do in hopes of preventing a cyberattack, then moves to a discussion of several potential solutions available to those businesses, and finally concludes with identifying the issue unique to entrepreneurs that is not practically available to startup enterprises in terms of risk management, leaving a meaningful dilemma in an age when small entrepreneurial enterprises often work to create many mobile apps and Internet platforms.

A. How Larger and Established Businesses Manage Cyber Risk

Although established, large businesses have a plethora of cybersecurity firms from whom the established businesses may purchase defenses against cyberattacks or cyberterrorism,[85] these businesses were the target of approximately 41% of spear-phishing attacks.[86] These options include offerings from newer companies such as CyberArk,[87] Palo Alto Networks,[88]

---

83 *E-stats 2013: Measuring the Electronic Economy*, U.S. CENSUS BUREAU (May 28, 2015), http://www.census.gov/econ/estats/e13-estats.pdf [http://perma.cc/XFP5-QN7H].

84 MCKINSEY GLOBAL INSTITUTE, MCKINSEY & CO., INTERNET MATTERS: THE NET'S SWEEPING IMPACT ON GROWTH, JOBS, AND PROSPERITY 16 (May 2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

85 Any meaningful discussion of natural person cyber protection generally resides beyond this Article's scope.

86 SYMANTEC, *supra* note 51, at 14.

87 *See* Renaissance Capital, *US IPO Pricing Recap: CyberArk Software Pops 85% and Year's Second Largest IPO Trades up*, NASDAQ (Sept. 28, 2014, 1:21 PM), http://www.nasdaq.com/article/us-ipo-pricing-recap-cyberark-software-pops-85-and-years-second-largest-ipo-trades-up-cm396042 [http://perma.cc/C6SD-GDLK]. Israel's CyberArk, although a foreign company, had its initial public offering ("IPO") on the United States' NASDAQ as recently as 2013, and saw its share price more than triple from June 2014 to June 2015. CyberArk—as a foreign cybersecurity company—does, however, raise the issue of allowing foreign corporations to collaborate with the U.S. government on cyberterrorism and cybersecurity and to what extent these collaborative efforts should go,

FireEye,[89] Rapid 7,[90] or established companies such as IBM[91] and Cisco.[92] Further, beyond cyber prevention and cyber clean-up companies, established businesses generally have the ability to obtain cybersecurity insurance.[93] Arca, a prominent exchange traded fund which holds stock of cybersecurity firms and trades under the ticker symbol "HACK" on the NYSE, has performed well relative to the broader markets since the ETF's inception.[94]

Cybersecurity insurance, while new and rare in its current form (it originated in the late-1990s in a different form because of different technological capabilities),[95] is expensive, potentially because of the difficult nature of quantifying risks[96] associated with cybercrime and cyber terror and because few large insurers offer the product.[97] AIG predicts that the cyber-insurance market

---

even with traditional U.S. allies.

88 *See* Palo Alto Networks, Inc., Annual Report (Form 10-K) *passim* (Sept. 18, 2014).

89 *See* FireEye, Inc., Annual Report (Form 10-K) 6 (Mar. 3, 2015). FireEye, Inc. advised on the famed 2013 Sony Breach. Basak, *supra* note 12, at 5.

90 *See* Rapid7, Inc., Amendment No. 1 to Form S-1 (Form S-1/A) 52 (June 26, 2015).

91 *See, e.g.*, *Cyber Security Solutions from IBM*, IBM, http://www-304.ibm.com/industries/publicsector/us/en/contentemplate1/!!/xmlid=148819 [http://perma.cc/UL58-7JUT] (marketing IBM's apparent "Cyber Security Solutions" and "Cyber Security Leadership"). *But see* Alex Barinka, *Five Charts Show Why IBM Is Worst Dow Stock for 2nd Year*, BLOOMBERG BUS. (Dec. 30, 2014, 12:43 PM), http://www.bloomberg.com/news/articles/2014-12-30/five-charts-show-why-ibm-is-worst-dow-performer-for-second-year [http://perma.cc/J4RU-ZGQE]; Kevin Kingsbury, *IBM Is One Week away from Infamy*, WALL ST. J.: MONEYBEAT (Dec. 24, 2014, 9:05 AM), http://blogs.wsj.com/moneybeat/2014/12/24/ibm-is-one-week-away-from-dow-infamy/ [http://perma.cc/G3T6-9HN8] ("IBM is just a week away from some infamy—becoming the first Dow component to be bottom of the barrel in consecutive years since now-departed Bethlehem Steel in 1995 and 1996."); *Heard on the Street: IBM Biggest Dow Loser for Second Year*, POST-BULLETIN (Dec. 31, 2014 4:38 PM), http://www.postbulletin.com/business/heard-on-the-street-ibm-biggest-dow-loser-for-second/article_834834c4-fe05-588e-bf1f-ee577be4c90f.html [http://perma.cc/SMM9-2F6J] (indicating collectively that IBM has been the worst performing Dow Jones Industrial Average component company for two years in a row in 2013 and 2014, a feat not accomplished since the mid-1990s, and IBM's white papers on information technology on IBM's website are typically from the decade ending 2010, with only one white paper in the past three years).

92 *See, e.g.*, *Cybersecurity*, CISCO, http://www.cisco.com/web/strategy/government/defense_cybersecurity.html [http://perma.cc/4PUG-RXDM] (indicating various industry-specific cybersecurity solutions).

93 Basak, *supra* note 12, at 2.

94 PureFunds ISE Cyber Security ETF, Supplement to the Prospectus dated Nov. 7, 2014 and Statement of Additional Information ("SAI") dated November 7, 2014, as supplemented March 24, 2015 (Form 497) (June 18, 2015).

95 Basak, *supra* note 12, at 3.

96 *Id.* ("Most firms are reluctant to offer policies for property damage resulting from hacking because there's almost no data available to determine costs . . . . Insurers have been excluding infrastructure damage caused by cyber-attacks from standard property and general liability policies, said Kevin Kalinich, who leads the cyber-risk team at insurance broker Aon Plc.").

97 *Id.* (indicating that, for example, Zurich Insurance Group, AG and Munich Re are considering offering these products but do not offer the product currently).

as of 2015 is $2 billion in annual premiums but could be $10 billion in annual premiums by 2020.[98]

Currently, coverage limits through AIG are at $100 million each for both property damage and bodily injury caused by a cyberattack.[99] Even if an established business were to pay the premiums for a cyber-insurance policy, these policies do not cover certain important cybersecurity matters, because of a lack of data on risk and cost.[100] To contextualize this lack of actuarial data, insurers currently have fewer than twenty years of data points from which to develop cyber-insurance policies, in comparison to up to one hundred years of data points from which to develop and tweak more typical property or liability insurance.[101]

B. The Financial Elephant in the Room: The Entrepreneurial Cost

Unlike established businesses, entrepreneurial startups are constantly concerned with so-called "runway" (the amount of time the company has before running out of cash),[102] burn rates (how quickly the company spends its cash),[103] and attracting new financial capital to allow the business to continue operating (one can think of this scenario as new equity investment equaling revenue for the entrepreneurial startup, often employing only a few people, typically at below-market cash consideration in return for equity stakes in the startup that have unlimited upside at the point of a successful exit, such as an acquisition or an IPO). And in 2014, small businesses were the target of 34% of spear-phishing attacks, only seven percentage points below those of large businesses,[104] an increase of more than 88% from 2011 levels.[105] Furthermore, according to the website of 2016 presidential candidate, former Florida Governor Jeb Bush, in 2014 "60% of all targeted attacks struck small and medium-sized organizations, *which often have fewer resources to invest in cybersecurity*."[106]

---

98 *Id.*

99 *Id.*

100 *Id.; see also Cyber Risk Assessments*, KROLL, http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments [http://perma.cc/T76A-6NEH] (describing assessing risk from well-known security-in-many-industries-firm, Kroll).

101 Basak, *supra* note 12, at 4.

102 *See, e.g.*, DAVID FEINLEIB, WHY STARTUPS FAIL: AND HOW YOURS CAN SUCCEED 33 (2012).

103 *See, e.g.*, EMERGING COMPANIES GUIDE, A RESOURCE FOR PROFESSIONALS AND ENTREPRENEURS 202–04 (Robert L. Brown & Alan S. Gutterman eds., 2d ed. 2004).

104 SYMANTEC, *supra* note 51, at 14.

105 *Id.* at 70 (indicating spear phishing of small businesses represented 18% of attacks in 2011 but 34% by 2014).

106 *Strengthening Cybersecurity*, JEB!2016 (Sept. 14, 2015), https://jeb2016.com/strengthening-cybersecurity/?lang=en [http://perma.cc/BF7G-G3FZ] (emphasis added).

This Article does not intend to convey that startups lack access to the choices available to established business discussed in Section II.A. Rather, startups often are unable to devote the financial resources necessary to these products because of runway, burn-rate, the pacing and amounts of attracting additional financial capital available to the enterprise, and the unknown costs associated with cybersecurity risk management.[107] The cost of complying with existing and proposed laws, regulations, and orders discussed in Part III is simply impossible for many entrepreneurial startups, whether due to the founders' ignorance of the governing rules or the inability to afford cyberthreat risk compliance, either financially or in terms of focus on growing the business.

As a result, a question exists for the reader throughout Part III, which is, "should entrepreneurial startups be faced with complying with the same regime as established corporations as described in Section II.A?"

III. FEDERAL LAWS, REGULATIONS, AND PROPOSED LEGISLATION

In early 2015, President Obama stated: "[I]n this dizzying age of technology and innovation . . . cyber-criminals . . . can . . . [t]urn your life upside down. It may take you months to get your finances back in order. . . . So this is a direct threat to the economic security of American families and we've got to stop it."[108] Elsewhere, President Obama indicated: "Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property."[109] Understanding some of what the government has proposed and already put in place is also necessary to

---

107 *See* VERIZON, *supra* note 9, at 27–28 ("When budgeting and operating an InfoSec [information security] program, accurately assessing . . . how much it'll cost [is] critically important. A lack of reliable estimates leads to a creative environment for decision making, where underspending, overspending, and useless spending invariably result."). Verizon estimated that the average financial loss from a cyber breach per 1000 records was between $52,000 and $87,000. Given that many angel investors typically provide startup capital to entrepreneurs in chunks of approximately $25,000–$50,000, seed-stage investment can be eliminated by a cyber breach, without even discussing the cost of cyber risk management. Even the predicted cost of only 100 records is over $25,000. *Id.*

108 *Remarks by the President at the Federal Trade Commission*, WHITE HOUSE (Jan. 12, 2015, 12:15 PM), https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission [http://perma.cc/GZT6-RZHQ]; *see also* Tau & Dwoskin, *supra* note 53 ("The proposals came amid the revelation the U.S. Central Command Twitter and YouTube accounts appeared to have been [hacked by Islamic militants], underscoring cybersecurity challenges the U.S. faces. The tweets posted by the hackers purportedly included phone numbers of top military commanders and claimed to provide military scenarios for a [potential] conflict with North Korea and China.").

109 *Foreign Policy Cyber Security*, WHITE HOUSE, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity [http://perma.cc/9JM4-NQ2M].

appreciating the entrepreneurial startup's perspective in terms of cybersecurity and cyberterrorism protection efforts. This Part describes several of those measures, including proposed and existing legislation and recent comments from regulatory agencies.

A. Proposed Legislation

Timed to coincide with the comments quoted in this Part's opening paragraph, at a speech delivered at the Federal Trade Commission ("FTC"), the Obama administration indicated that it would be introducing legislation of varying sorts with the hope of protecting consumers from cyberattacks.[110] These proposals generally aimed at protecting privacy, preventing identity theft, and helping children remain safe in cyberspace. The following day, the President announced additional proposals at DHS.[111]

There, President Obama discussed how the federal government could "work with the private sector to better protect American companies against cyber threats."[112] The President further indicated: "Foreign governments, criminals and hackers probe America's computer networks every single day. We saw that again with the attack at Sony, which actually destroyed data and computer hardware that is going to be very costly for that company to clean up."[113]

These proposals were added to the President's 2013 Executive Order 13636, which—issued exactly two years to the week before the 2015 proposals—concerned cyberthreats, including cyberterrorist threats, to the nation's infrastructure.[114] Yet, as of October 2015, the cybersecurity web page at whitehouse.gov had no updates—text or video—since May 1, 2015, well before the numerous cyberattacks described earlier in this Article.[115]

B. SEC and FINRA

From a business perspective, perhaps the next most relevant guidance comes from the Securities and Exchange Commission

---

110 *Remarks by the President at the Federal Trade Commission*, *supra* note 108.

111 *Remarks by the President at the National Cybersecurity Communications Integration Center*, WHITE HOUSE (Jan. 13, 2015, 3:10 PM), https://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent [http://perma.cc/XP7B-326J].

112 *Id.*

113 *Id.*

114 *Executive Order -- Improving Critical Infrastructure Cybersecurity*, WHITE HOUSE (Jan. 12, 2015), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [http://perma.cc/U2YE-RD6B].

115 *Foreign Policy Cyber Security*, *supra* note 109.

("SEC") and Financial Industry Regulatory Authority ("FINRA"). In 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") examined approximately fifty broker-dealers ("B/Ds") and fifty registered investment advisers ("RIAs").[116] OCIE's ultimate report indicated that a majority of B/Ds and RIAs examined maintained written information security policies ("WISPs"), nearly half of those firms examined identified industry cybersecurity practices via peer groups or information sharing, and more than 90% of B/Ds and RIAs employed some sort of encryption. These data points resulted from participating firms answering questionnaires, not from any inspection or testing by OCIE or a designated third-party to act on OCIE's behalf.[117]

FINRA's report described what the organization not only viewed as the material cybersecurity risks facing B/Ds but also believed were appropriate risk mitigation tactics, including references to the NIST framework.[118] The report identified risk assessment and oversight of third-party vendors ("vendor management"), consultants, and others, as a material concern for B/Ds.[119] Currently, however, neither B/Ds nor RIAs are under any SEC requirement to maintain cyberthreat insurance or have written policies regarding customer losses in the event of a cyber breach.

C. The SAFETY Act

The so-called "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" ("SAFETY Act")[120] provides, in essence, a shield for certain businesses from tort liability. Specifically, the SAFETY Act provides a safe harbor—in the form of an indemnity—to cybersecurity businesses that fail in their essential function of providing cybersecurity.[121] While this Article focuses on the indemnity provision, as authors Finch and Spiegel

---

116 Office of Compliance Inspections and Examinations, U.S. Securities & Exchange Commission, *Cybersecurity Examination Sweep Summary*, 4 NAT'L EXAM PROGRAM RISK ALERT (Feb. 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf [http://perma.cc/BKM8-BF6Q].

117 Anthony Zeoli, *Lock It up: SEC & FINRA Weigh in on Cybersecurity Issues* (Feb. 23, 2015, 10:09 PM), http://www.crowdfundinsider.com/2015/02/63237-lock-it-up-sec-finra-weigh-in-on-cybersecurity-issues/ [http://perma.cc/A4MT-UKJE].

118 FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 42–43 (2015). For more on the National Institute of Standards and Technology (NIST), see NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, www.nist.gov [http://perma.cc/E8HW-YKXR].

119 FIN. INDUS. REGULATORY AUTH., *supra* note 118.

120 Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, 6 U.S.C. §§ 441–444 (2012) [hereinafter *SAFETY Act*].

121 After *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010), if corporations are persons, then the word that attaches to describe corporations is "who," not "that."

asserted: "These liability protections can take the form of jurisdictional defenses, a cap on liability, or a presumption of immediate dismissal of third-party liability claims."[122]

In addition, the SAFETY Act permits the federal government to give a seal of approval to certain entities (very similar to the FTC's COPPA compliance seal, despite negotiable prices and hacks that occurred and despite Target having been COPPA compliant). These entities receive a certification as a "Qualified Anti-Terrorism Technology" or "QATT."[123] The SAFETY Act mandates that all cyberterrorism-related liability claims must be litigated in federal court; punitive damages and pre-judgment interest awards are barred; and compensatory damages are capped at an amount agreed to by both the government and company, with the damage cap equal to a set amount of insurance the company must possess. Further, damages awarded to plaintiffs will be offset by any collateral recoveries they receive (e.g., victim compensation funds, life insurance, etc.).[124]

As Finch and Spiegel asserted: "The only way this presumption of immunity can be overcome is to demonstrate that the application contained information that was submitted through fraud or willful misconduct."[125] Cyberattacks are governed by the SAFETY Act's definition of "terrorism," regardless of the type of product or service in which the business is engaged (i.e., the business does not have to be in the technology space for these protections to apply). However, any client who purchases QATT-approved software from a certified QATT seller is absolved from any liability, so long as an act of terrorism is declared by the Secretary of Homeland Security.[126]

Simply put, the seller of the QATT is the sole look-to for liability, and the DHS painstakingly articulated this fact when

---

122 Brian E. Finch & Leslie H. Spiegel, *Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety* Act, 30 SANTA CLARA HIGH TECH. L.J. 349, 351 (2014).

123 *SAFETY Act*, 6 U.S.C. §§ 441–444 (detailing QATT).

124 *Id.* § 442.

125 Finch & Spiegel, *supra* note 122, at 369 (referencing the regulations implementing the *SAFETY Act* of 2002, 71 Fed. Reg. 33147, 33150 (June 8, 2006) (codified in 6 C.F.R. pt. 25)); s*ee also* 6 U.S.C. § 444(2)(b).

126 The *SAFETY Act* states:

> There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. . . . Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers.

6 U.S.C. § 442(a)(1) (2012).

promulgating the final rule implementing the SAFETY Act.[127] Practically, the SAFETY Act supersedes the existing bankruptcy system and replaces an entire body of law with an explicit government grant to internalize arguably nominal costs for large businesses who can afford to purchase QATT-approved software, raising the question of whether entrepreneurial startups are able to purchase QATT-approved software, and externalizing the tremendous damage that could occur should a cyber-terror attack happen to a given safe-harbored business.

D. Discussion of Policy Prescriptions Generally

Typically, a law journal article identifies a problem and then attempts to propose a unique solution underpinned by a proposed law, rule, regulation, executive order or the like. However, as Scott Kannry, the CEO of Aon Global in the insurance industry—the holder of both a J.D. and M.B.A.—has stated:

> [Saying that the cybersecurity industry is] [f]ailing isn't the right description, although one could easily come to that conclusion given the trend line on events over the past 12 months. I would characterize the industry as one that needs a better approach. To date, most of the focus has been on solutions –firewalls, encryption, antivirus, you name it. The problem is that a cyber security program consists of dozens, if not hundreds of technologies, policies and procedures, none of which is a silver bullet and any of which can be immediately outdated based on the ever evolving risk climate. Imagine if your job was solely focused on putting together a puzzle, but some pieces were missing, others didn't fit together, and every 30 minutes the board changed. Technically, you would fail, but you never really stood a chance![128]

As a result, current cybersecurity policies appear too lax; the question is how the public and private sector should procedurally and substantively build an effective framework.

---

127 Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, 71 Fed. Reg. at 33150–51 ("Congress balanced the need to provide recovery to plaintiffs against the need to ensure adequate deployment of anti-terrorism technologies by creating a cause of action that provides a certain level of recovery against Sellers, while at the same time protecting others in the supply chain."); *see also* 6 C.F.R. § 25.7(d) (2016) ("There shall exist only one cause of action for loss of property, personal injury, or death for performance or non-performance of the Seller's Qualified Anti-Terrorism Technology in relation to an Act of Terrorism. Such cause of action may be brought only against the Seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyers, the buyers' contractors, or downstream users of the Technology, the Seller's suppliers or contractors, or any other person or entity.").

128 Christopher P. Skroupa, *The Insurance Industry's Unique Vantage Point on Cyber Security*, FORBES (July 9, 2015, 5:42 PM), http://www.forbes.com/sites/christopherskroupa/2015/07/09/the-insurance-industrys-unique-vantage-point-on-cyber-security/.

IV. EVIDENCE THAT A PUBLIC-PRIVATE OR PRIVATE MARKET ALTERNATIVE EXISTS

In his January 2015 remarks to DHS, President Obama indicated that "[n]either government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand-in-hand as partners."[129] This Part explores that option, with an eye toward the entrepreneurial startup.

Yet, as this Article indicated above, many of the available cyber-protection solutions—whether software or insurance, regardless of not only the size of the enterprise offering the cyber protection but also the QATT-approval safe harbor involvement—are simply too expensive for entrepreneurial startups concerned with burn rate, runway, and continuing capital raises while protecting against founder and insider equity dilution.

For example, the sole government resource that appears to exist for small businesses, of which entrepreneurial startups are a flavor, is the Federal Communication Commission's ("FCC's") "Small Biz Cyber Planner 2.0."[130] And version 2.0 was launched three years ago in October 2012, which, going back to Moore's Law,[131] likely means that the Cyber Planner is out of date, despite the FCC's stated goal of providing "an online resource to help small businesses create customized cybersecurity plans."[132] "As larger companies take steps to secure their systems, less secure small businesses are easier targets for cyber criminals."[133]

The planner itself is a fifty-one page booklet (also customizable for a business on the FCC's website, but all information comes directly from the booklet) that includes sections such as (1) inventory your data; (2) keep a record of the data's location, and move the record to more appropriate places when needed; (3) develop a privacy policy; (4) protect data collected on the Internet (stating "you need to make sure any data collected through your website and stored by the third party is sufficiently secure," as if that level of due diligence is necessarily feasible); (5) create layers of security; (6) plan for data loss or theft (threateningly stating "[n]ot only can the loss or theft of data hurt your business, brand and customer confidence,

---

129 Air Force Tech. Sgt. Jake Richmond, *Obama Unveils Next Steps in Cybersecurity Plan,* U.S. DEP'T DEF. (Jan. 13, 2015), http://www.defense.gov/News-Article-View/Article/603919 [http://perma.cc/SXL2-9DR6].

130 *Cyberplanner*, FED. COMM. COMMISSION, https://www.fcc.gov/cyberplanner [http://perma.cc/GRD5-7BYL].

131 *See* Harsha, *supra* note 2.

132 *Cyberplanner*, *supra* note 130.

133 *Id.*

it can also expose you to the often-costly state and federal regulations that cover data protection and privacy. Data loss can also expose businesses to significant litigation risk").[134] Whether entrepreneurs even have the time to read this material is questionable, given that founders must essentially dedicate all of their waking hours to their fledgling businesses. The FCC also provides arguably meaningful guidance to protect mobile wallets, which employ software downloaded to a mobile device to pay for commercial transactions or person-to-person payments.[135] The advice provided in this booklet is of questionable value in functioning as a cyber safeguard.

As a result, entrepreneurial startups face unique challenges when faced with defending their firms from hackers, cybercriminals, cyberterrorists, and others attempting to successfully breach data, big data, or systems, via the Internet or the Internet of Things, negatively affecting the startups, including to the point of the startups' very existences. Part V advances some initial proposals for further discussion and evaluation that would assist the entrepreneurial startup when dealing with the very real threats that face entrepreneurs.

V. PROPOSED INITIAL DISCUSSION POINTS FOR ENTREPRENEURIAL SUCCESS FACING CYBERTHREATS

This Part asserts several proposals that may be both cost efficient and effective for the startup and effective for the startup's consumer base. First, communication and cooperation between the public and private sector are important.[136] Having said that, much of corporate law—beyond securities regulation, taxation, consumer protection, and immigrant worker visas—concerning entrepreneurial startups resides at the state level. From entity formation to the applicable internal affairs doctrine affecting the startup, to terms of use for many apps and web platforms, the end-user must agree to specific state law for applicable law, jurisdiction, and forum. Because of state law's importance, the proposals in this Part reflect suggestions for state-level changes to corporate codes, rather than action on the part of federal agencies.

---

134 *Cyber Security Planning Guide*, FED. COMM. COMMISSION PDS-1–PDS-5, https://transition.fcc.gov/cyber/cyberplanner.pdf [http://perma.cc/ZW8V-4PAQ]; *see also FCC Smartphone Security Checker*, FED. COMM. COMMISSION, https://www.fcc.gov/smartphone-security [http://perma.cc/T8CW-Y6AQ] (last updated Oct. 30, 2015, 12:45 PM).

135 *Mobile Wallet Services Protection*, FED. COMM. COMMISSION, https://www.fcc.gov/guides/mobile-wallet-services-protection [http://perma.cc/T7F6-FCY5] (last updated Nov. 4, 2015, 12:00 AM).

136 *See* Basak, *supra* note 12.

A. Corporate Governance

Ultimately, corporations are governed by a board of directors.[137] Corporate boards have fiduciary duties of care (unless exculpated) and loyalty to the company and shareholders.[138] One proposal is that a part of the duty of care that cannot be exculpated is that each corporation must create a functioning risk management committee, under whose umbrella falls cybersecurity. For public companies, the SEC could take the position that, similar to the Sarbanes-Oxley-mandated requirement of an audit committee expert serving on the audit committee, an IT or risk management expert serve on that committee. I would prefer to see such requirements come from the state-level so that businesses can choose what governance framework works best for them among a variety of cybersecurity fiduciary risk management options. For entrepreneurial startups advised appropriately, the fear of personal liability for breaching the fiduciary of care should be sufficient incentive to create a risk-management committee, without the added need and cost of an IT expert serving on the committee. People tend to respond to incentives, and the incentive of facing unlimited personal liability for a fiduciary duty breach should encourage many entrepreneurial startups to create a risk-management committee.

B. Sliding Scales for Size

To avoid disincentivizing entrepreneurial startups from forming while balancing the need to operate in a riskless manner, a sliding scale for liability could exist. This Article stipulates that little to no logical reason exists for many arbitrary numbers that laws and regulations use relative to requirements and exemptions for corporations, based on either financial or employee pool size. Having said that, this Article does advance that appropriately tailored safe harbors from liability should exist for businesses with an equity capitalization under an inflation-adjusted amount of, hypothetically, $100 million, those entities with fewer than, somewhere near twenty employees, and newly formed entities fewer than approximately thirteen months in age that are non-affiliates of previously existing enterprises.

With the rapid pace that entrepreneurial startups must deploy capital for research and development, alpha testing, beta testing, a focus on obtaining additional capital from angel or

---

137 A discussion of LLCs or the array of other owner-liability-shielded entities is beyond the scope of this Article.

138 *See generally* D. GORDON SMITH & CYNTHIA A. WILLIAMS, BUSINESS ORGANIZATIONS (2d ed. 2004).

venture capital investors (or both), seed stage companies often lack the time and human and financial capital to employ attorneys to advise them of the need for cyber-risk assessments. This Article does not believe that it is effective policy to kill off fledgling businesses that are cyberhacked, because those companies simply lacked the knowledge, the resources, or the time because of their nascent nature. As the businesses grow in size, time of existence, and financial capital, then sliding scales of obligations should begin to fall on the entrepreneurial ventures.

These matters could be self-regulating, for example, by the Venture Capital Association of America or other similar groups affecting the startup ecosystem. What fund manager would want to deploy venture or seed-stage capital to an enterprise that was naked in the face of cyber risk? Couple this self-regulation with tweaking of existing state statutes on fiduciary duties that would require an organization to face risk management of cybersecurity in its evaluation of fiduciary duty exculpation at entity formation, and the private sector can self-regulate for entrepreneurs.

C. Private-Public Partnering of Cyber Insurance for Startups

Protecting startups should not, however, come at the expense of consumers. As a result, affordable and meaningful cyber insurance could be required by states. A need for this insurance exists, as articulated earlier in this Article, but costs are high and insurers lack the actuarial data that they need. State-level, or if absolutely necessary, federal level, cyber-terror or cyberthreat insurance could be mandated and overseen by a government insurance agency, such as the Federal Deposit Insurance Corporation ("FDIC") or Pension Benefit Guaranty Corporation ("PBGC"). While, for example, the PBGC has protected the pensions of millions of Americans since the entities formation under ERISA in the mid-1970s, PBGC is funded by the companies whose pension plans it insures, rather than the taxpaying public, and claimants are paid based on a sliding scale based on financial capital. A similar framework may work well in the case of protecting customers of startup enterprises from financial loss, and the insurance and administration of the insurance may be at a lower cost than currently exists in the marketplace.

CONCLUSION

In mid-October 2015 at the first Democratic Party presidential debate, moderator Anderson Cooper asked: "[w]hat is the greatest national security threat to the United States?"

Out of five candidates—among whom were four senators, two governors, a former secretary of state, and a former secretary of the Navy—only one candidate, attorney, former Navy secretary, and Senator Jim Webb, responded with "cyberthreats." Webb indicated: "Our greatest day-to-day threat is cyber warfare against this country."[139]

Regardless of whether former Senator Webb is correct in his assessment of the single greatest security threat to the United States, cyber terror and cybersecurity are legitimate emerging threats to this nation. And in the face of those threats, this Article has proposed problems and policy solutions specific to protecting this country's citizenry from cyberattacks on businesses, with an emphasis on the specific challenges faced by entrepreneurial startups in that effort that are far different than the challenges faced by established businesses in the hopes of spurring a dialogue at this Symposium that both protects the U.S. populace and remains supportive of ensuring an environment supportive of entrepreneurial startups from ideation to commercialization.

139 *CNN Democratic Debate – Full Transcript*, CNN (Oct. 13, 2015, 11:26 PM), http://cnnpressroom.blogs.cnn.com/2015/10/13/cnn-democratic-debate-full-transcript/ [http://perma.cc/66UV-EN6J].