Winter 2018

How Much Should We Spend to Protect Privacy?: Data Breaches and the Need for Information We Do Not Have

Richard Warner

Robert H. Sloan, *University of Illinois at Chicago*

HOW MUCH SHOULD WE SPEND TO PROTECT PRIVACY?: DATA BREACHES AND THE NEED FOR INFORMATION WE DO NOT HAVE

Robert H. Sloan and Richard Warner***

INTRODUCTION

A cost/benefit analysis approach to privacy concerns raises two tradeoff issues. One is making appropriate tradeoffs between privacy and the many goals served by the collection, distribution, and use of information. The other is making tradeoffs between investments in security, that is, in preventing unauthorized access to information, and a variety of other goals. Much has been written about the first tradeoff. We focus on the second. The issue is critical. Data breaches occur at the rate of over three a day.¹ The aggregate social cost is high. One recent study puts the average cost of a breach for a business at \$4 million.² Such estimates are controversial,³ but it is clear that breaches impose significant losses on businesses,⁴

* Professor and Head, Department of Computer Science, University of Illinois at Chicago. Partially supported by National Science Foundation Grant No. DGE-1069311.

** Professor of Law, Chicago-Kent College of Law, Visiting Foreign Professor, University of Gdańsk, Poland.

¹ IDENTITY THEFT RESOURCE CENTER, *Data Breaches*, <https://www.idtheftcenter.org/data-breaches/> (last viewed Dec. 4, 2018). The Identify Theft Resource Center (ITRC) uses a narrow definition of a breach: a data breach is “an incident in which an individual name plus a Social Security number, driver’s license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure.” Unauthorized access to computers and networks can be “potentially put at risk because of exposure” a great deal of other sorts of sensitive information, so data breaches would be even more common on the correspondingly broader understanding of breach. Whatever the exact breach rate, there are enough breaches to impose significant costs on society.

² PONEMON INST., *COST OF DATA BREACH STUDY: GLOBAL ANALYSIS* (2016), <https://www.ibm.com/security/data-breach/> [hereinafter *Cost of Data Breach Study*]. That \$4 million is Ponemon’s estimate of *data breach* costs as defined in the study and is up from its estimates in previous years. Its 2015 study of *cybercrime* costs defines those costs more broadly and estimates them at \$7.7 million per business annually. PONEMON INST., *2015 COST OF CYBER CRIME STUDY: GLOBAL ANALYSIS* (2015), http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

³ See, e.g., Maria Korolov, *\$154 or 58 cents -- what’s the real cost of a breached data record?*, CSO ONLINE (Jun 5., 2015, 6:29 AM), <http://www.csoonline.com/article/2931839/data-breach/154-or-58-cents-whats-the-real-cost-of-a-breached-data-record.html>.

⁴ In 2014, the aggregate loss in the United States from identity theft was around \$15.4 billion. Erika Harrell, *Victims of Identity Theft, 2014* 7 (Bureau of Just. Stat., Sept. 2015), <https://www.bjs.gov/content/pub/pdf/vit14.pdf>. Earlier United States estimates of the cost of identity

consumers,⁵ and society.⁶ Security experts have long explained how to better defend against security breaches.⁷ So, why does society tolerate a significant loss that it has the means to avoid?

Some may object that society does *not* tolerate breaches. After all, laws—current and proposed—impose requirements aimed at improving information security. However, there are information security laws that “obligate companies to establish and maintain ‘reasonable’ or ‘appropriate’ security procedures, controls, safeguards, or measures, but give no further direction or guidance.”⁸ The courts have not clarified the situation; there are no cases that establish what standards of care an organization must adopt with regard to data security.⁹

theft alone are also in the billions. For a summary of relevant studies, see Fred H. Cate, *Information Security Breaches and the Threat to Consumers* 6, (Ctr. for Info. Pol’y Leadership at Hunton & Williams, Sept. 2005), <http://www.repository.law.indiana.edu/facpub/1291> (reporting 10.1 million victims of identity theft in 2003 and total losses to consumers of over 50 billion). Identity theft estimates ignore non-identity theft losses from, for example, ransomware, denial of services attacks, botnets engaged in fraud and other illegal activities, and viruses. A United Kingdom government study with a broader focus estimates the yearly cost of data breaches to be £21bn to businesses, £2.2bn to government and £3.1bn to citizens. DETICA, *THE COST OF CYBERCRIME 2* (Feb. 2011), <http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf>. For a follow-up study, see Ross Anderson et al., *Measuring the Cost of Cybercrime*, (Eleventh Workshop on Econ. of Info. Security, 2012), http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf.

⁵ Lillian Ablon et al., *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, (Rand Corp., 2016), https://www.rand.org/pubs/research_reports/RR1187.html.

⁶ Society as a whole incurs costs as businesses and consumers spend time and effort responding to data breaches instead of directing that time and effort toward more productive ends. Governments also incur costs from funding criminal enforcement efforts and from the taxes they would have collected on revenue from projects that were not undertaken because the funding for them was spent on responding to data breaches.

⁷ There are numerous undergraduate and graduate textbooks on computer security discussing how best to defend. See, e.g., ROSS J. ANDERSON, *SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS* (2nd ed. 2008); CHARLES P. PFLEEGER, SHARI LAWRENCE PFLEEGER & JONATHAN MARGULIES, *SECURITY IN COMPUTING* (5th ed. 2015); WILLIAM STALLINGS & LAWRIE BROWN, *COMPUTER SECURITY: PRINCIPLES AND PRACTICE* (3rd ed. 2014); WILLIAM STALLINGS, *NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS* (6th ed. 2016). Both the SANS institute and Australian Department of Defense publish fairly short lists of critical security controls, and the Australian Department of Defense argues that simply adopting its top four would vastly improve the information security posture of most organizations, eliminating about 85 percent of all incidents. See, e.g., Australian Cyber Security Centre, *Strategies to Mitigate Cyber Security Incidents*, <https://acsc.gov.au/infosec/mitigationstrategies.htm> (last visited Dec. 4, 2018); SANS Institute, *The CIS Critical Security Controls for Effective Cyber Defense*, <http://www.sans.org/critical-security-controls/> (last visited Dec. 4, 2018).

⁸ Thomas J. Smedinghoff, *Defining the Legal Standard for Information Security: What Does “Reasonable” Security Really Mean?*, *SECURING PRIVACY IN THE INTERNET AGE* 19, 23 (Chander, Gelman & Radin eds., 2008).

⁹ Mark C. Mao, Ronald I. Raether, Jr. & Sheila M. Pham, *Data Privacy: The Current Legal Landscape* 9 (Troutman Sanders LLP, 2016),

Laws currently fail to provide an adequate incentive to improve information security. Why? One answer is that they fail to provide sufficient detail about what counts as reasonable precautions against data breaches. That answer is more wrong than right. Perhaps greater detail is called for in some cases, but the more fundamental problem is that businesses lack sufficient information to make the cost/benefit judgments on which reasonableness in this context largely depend. An essential part of adequately defending online data is ensuring that business have the necessary information.

In Section I, we distinguish between businesses protecting consumers from data breach losses and businesses protecting themselves from those losses. We focus on the latter in this section and identify three problems that partially explain businesses' poor self-defense. Only one of those problems, vulnerabilities in networks, raises lack of information concerns. We focus on that problem in Sections II to V. We turn to the defense of consumers in Section II. We argue that businesses should bear a considerable part of the defensive burden, and that they are unlikely to do so with some form of legal liability for consumer losses. We also argue, however, that imposing legal liability will be ineffective without a solution to the lack of information problem that plagues businesses' self-defense. Section III considers ways of improving data breach defenses without immediately acquiring the necessary information about data breaches. We consider relying on expert opinions, outsourcing security, and data breach notification laws. None of those items are fully adequate as a solution to defending against data breaches. Section IV proposes a regime of mandatory anonymous reporting of relevant information about data breaches.

I. INADEQUATE DEFENSE

Businesses fail to defend adequately against data breaches on two fronts. They fail to adequately defend consumers, and they fail to adequately defend themselves. The failure to defend consumers is hardly surprising. The problem is, of course, negative externalities. Profit driven businesses ignore customers' and third-parties' losses, unless those losses also impose significant losses on the business.¹⁰ The point applies to cybersecurity. Organizations have

insufficient incentives to invest in strong data security and accountable privacy practices because, in essence, they didn't have to. Consider that lost or "stolen" customer or employee data often does not deprive an organ-

https://www.troutmansanders.com/files/Uploads/Documents/TS_Article_DataPrivacy-TheCurrentLegalLandscape_OCT_2016.pdf.

¹⁰ Benjamin Dean et al., *Sorry Consumers, Companies Have Little Incentive to Invest in Better Cybersecurity*, QUARTZ (Mar. 5, 2015), <http://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/>.

ization of its continued availability or use, as would loss or theft of physical property. Further, the (negative) consequences of poor security and mis-used data fall mainly if not entirely upon individual victims, often at a later date.¹¹

The result is that businesses fail to adequately approximate the following *consumer risk management goal*: choose the most effective defense meeting the condition that the defense investment is not greater than the expected consumer losses thereby avoided (over some appropriate time period).¹² We address the failure to defend consumers in Section II. This section considers business *self-defense*. The self-defense failure reveals the critical lack of information needed for adequate defense, and that same failure also plagues the defense of consumers.

A. *Business Self-Defense*

Businesses' self-defense is typically inadequate. As one commentator summed up the situation, "the bad guys basically go where they want to go and do what they want to do, and they're not being stopped. Maybe for every one organization that's effectively stopping attacks, there are 100 that are being breached."¹³ Why is this happening? The puzzle is that the profit maximizing approach is to pursue the following *business risk management goal*: choose the most effective defense meeting this condition—the defense cost is not greater than expected business losses thereby avoided (over some appropriate short- or long-term time period).¹⁴

Why do businesses typically fail—and often fail badly—to meet the business risk management goal? There are different answers for different problems. The problems correspond, more or less, to three types of vulnerabilities. A vulnerability is a property of a program, computer, or network that hackers can exploit to gain unauthorized access. We divide vulnera-

¹¹ Ann Cavoukian, *A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight* 5-6 (Eight Workshop on Econ. of Info. Security, 2009), https://www.ipc.on.ca/wp-content/uploads/Resources/privacy_externalities.pdf.

¹² Expected losses are the (estimated) actual losses discounted by the probability of their occurrence. For our purposes, it does not matter whether one interprets probability "objectively" as frequencies of occurrence or "subjectively" as degrees of belief. For an excellent discussion of the types of probability, see IAN HACKING, *AN INTRODUCTION TO PROBABILITY AND INDUCTIVE LOGIC* (2001).

¹³ George V. Hulme, *Security Spending Continues to Run a Step Behind the Threats*, CSO ONLINE (Oct. 16, 2013, 8:00 AM), <http://www.csoonline.com/article/2134074/strategic-planning-erm/security-spending-continues-to-run-a-step-behind-the-threats.html>.

¹⁴ Implementing this strategy faces significant problems in practice. It can be difficult to evaluate the effectiveness of various security measures. Relevant costs and benefits may not be quantifiable, and those that are may only be roughly and approximately so. In addition, costs and benefits may be quite difficult to predict.

bilities into these groups: software, human, and network. We focus on networks, as that is where the critical need for information arises.

B. *Three Types of Vulnerabilities, Three Different Problems*

1. Software Vulnerabilities

Mass-market software programs currently contain an unacceptable number of vulnerabilities. That is not inevitable. Software engineers know how to minimize, though alas not how to totally eliminate, vulnerabilities.¹⁵ How to write individual computer programs well, and the basics of software engineering are fairly well-settled subjects.¹⁶ The basics of high-quality code construction and software engineering generally form a significant fraction of the required core portion of the model computer science bachelor's degree curriculum jointly published by the two main professional societies for computer science in 2013,¹⁷ and in earlier model curricula.¹⁸

¹⁵ Software is different from other engineered products in that sufficiently complex software inevitably has some programming flaws. As far back as the 1980s, a panel convened to study the issues with software for President Reagan's Strategic Defense Initiative noted, "Simply because of its inevitable large size, the software capable of performing the battle management task for strategic defense will contain errors. *All systems of useful complexity contain software errors.*" STRATEGIC DEF. INITIATIVE ORG., DEP'T OF DEF., 19980819-140, EASTPORT STUDY GROUP: SUMMER STUDY 1985, A REPORT TO THE DIRECTOR, 14 (1985), <http://www.dtic.mil/dtic/tr/fulltext/u2/a351613.pdf> (emphasis added). Software engineering expert Capers Jones notes that one goal of software engineering best practices is to increase the percentage of bugs removed prior to delivery from 85 percent to something that "approach[es] 99 percent," (*not* that it approaches 100 percent). CAPERS JONES, SOFTWARE ENGINEERING BEST PRACTICES: LESSONS FROM SUCCESSFUL PROJECTS IN THE TOP COMPANIES xxvi (2010). In contrast, design flaws are not inevitable in, for example, refrigerators, batteries, and bridges even when they exhibit considerable complexity. Software alone combines complexity and inevitable flaws. Thus, no matter how much one invests in development procedures designed to reduce programming flaws, flaws—and perhaps vulnerabilities—will remain.

¹⁶ However, the choice of *which* software engineering methodology is the best one for managing various sorts of projects is contentious. In particular, there is debate about the relative merits of a traditional methodology called the Waterfall Model, with its origins in the late 1960s, versus various other methodologies, such as Spiral or Agile. See, e.g., David L. Parnas, *A Rational Design Process: How and Why to Fake it* 3, <http://www.cs.tufts.edu/~nr/cs257/archive/david-parnas/fake-it.pdf> (criticizing the Waterfall Model); Kent Beck et al., *Manifesto for Agile Software Development* (2001), <http://agilemanifesto.org/> (outlining the Agile Model).

¹⁷ JOINT TASK FORCE ON COMPUTING CURRICULA, ASS'N FOR COMPUTING MACHINERY, IEEE COMPUTER SOC'Y, COMPUTER SCIENCE CURRICULA 2013: CURRICULUM GUIDELINES FOR UNDERGRADUATE DEGREE PROGRAMS IN COMPUTER SCIENCE (2013), https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf.

¹⁸ See, e.g., JOINT TASK FORCE ON COMPUTING CURRICULA, ASS'N FOR COMPUTING MACHINERY, IEEE COMPUTER SOC'Y, COMPUTING CURRICULA 2001: COMPUTER SCIENCE (2001), <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2001.pdf>.

Years of studies confirm the common wisdom among experts in software development that proper attention to software development leads to lower defect rates.¹⁹ So why is software so full of vulnerabilities? In large part because reducing vulnerabilities requires a longer and more costly development process. Consumers have been unwilling to pay for the added value of security through slightly higher retail prices and companies, dependent on consumer sales, don't offer what consumers don't want. "Businesses are profit-making ventures, so they make decisions based on both short- and long-term profitability,"²⁰ and the "market often rewards first-to-sell and lowest cost rather than extra time and cost in development."²¹ The typical profit-maximizing strategy is to keep costs down and be the first to offer a particular type of software, even if it is imperfect in a variety of ways, including having vulnerabilities.²² We discuss software vulnerabilities and a possible remedy in detail elsewhere.²³

2. Human Vulnerabilities

The main human vulnerability is the human propensity to trust. Think of human vulnerabilities as an unwitting invitation to enter. Vampire movies are a nice analogy. In classic vampire movies, vampires can't enter a house unless invited in, so the audience cringes when some innocent person unwittingly asks the obvious-to-the-audience vampire to cross the threshold. Far too many invite hackers to cross the thresholds of their computers and networks allowing them to gain "access to buildings, systems or data

¹⁹ See generally Anthony Hall, *Seven Myths of Formal Methods*, 7 IEEE SOFTWARE 11, 11–19 (Sept. 1990) (discussing Praxis studies and the CASE project). See also I. J. Hayes, *Applying Formal Specification to Software Development in Industry*, SE-11 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 169, 175–76 (Feb. 1985) (discussing the usefulness of software engineering techniques in some particular projects); Alan MacCormack et al., *Trade-offs Between Productivity and Quality in Selecting Software Development Practices*, 20 IEEE SOFTWARE 78, 81–84 (Sept.–Oct. 2003) (comparing various software engineering techniques).

²⁰ Bruce Schneier, *Information Security and Externalities*, SCHNEIER ON SECURITY (Jan. 2007), https://www.schneier.com/essays/archives/2007/01/information_security_1.html.

²¹ Eugene H. Spafford, *Remembrances of Things Pest*, 53 COMM. ACM 35, 36 (2010).

²² See generally C. SHAPIRO & H. R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 50–51 (1999). The economics and information security community has developed Shapiro and Varian's initial insights. Much of this work has been reported in the annual Workshop on the Economics of Information Security since 2002. For information on the workshops from 2002 to 2010, see <http://weis2010.econinfosec.org/index.html>. For a good general survey, see Ross Anderson & Tyler Moore, *Information Security: Where Computer Science, Economics and Psychology Meet*, 367 PHIL. TRANSACTIONS ROYAL SOC'Y A 2717, 2721–22 (2009).

²³ See ROBERT H. SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND INFORMATION SECURITY (2013); Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, 2012 UNIV. ILL. J. TECHNOL. LAW POLICY 45 (2012).

by exploiting human psychology.”²⁴ Phishing is a good example. Phishing is the use of an electronic communication that masquerades as being from someone trustworthy in order to gain unauthorized access to information. For example, in a case study entitled, “Examining how a China-based threat actor stole vast amounts of PII,” Mandiant notes that:

Phishing attacks continue to be a theme year after year, and this case is no different. It began with a threat actor successfully enticing a user to follow a malicious link in a phishing email. The link downloaded a backdoor, providing the threat actor access to the victim’s environment. Once the threat actor obtained a foothold, the reconnaissance activity was primarily centered on the identification of databases with the greatest volume of PII.²⁵

Phishing is by no means the only way hackers masquerade themselves to exploit people’s trust. Other examples include various other forms of social engineering²⁶ and Trojan horses.²⁷

3. Vulnerabilities in Networks

The way to reduce human vulnerabilities is hardly a mystery. It is primarily a matter of adequate education and training.

There is no small set of vulnerabilities that accounts for all or most of the data breaches. Recent data breaches involve, among other things, mis-configured vendor access,²⁸ lack of encryption of data in motion,²⁹ lack of encryption of data at rest,³⁰ lack of basic use of firewalls,³¹ and vulnerabilities in non-mass market infrastructure software. In the case of the Target

²⁴ George V. Hulme & Joan Goodchild, *What is Social Engineering? How Criminals Take Advantage of Human Behavior*, CSO ONLINE (Aug. 3, 2017, 6:31 AM), <https://www.csoonline.com/article/2124681/social-engineering/security-awareness-social-engineering-the-basics.html>.

²⁵ MANDIANT, *M-TRENDS 2016* 17 (2016), <https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2016-mtrends.html>.

²⁶ Social engineering is pretending to be someone else in order to gain access to a computer or network, or, more generally, to obtain any confidential information. Skip tracers (professionals specializing in locating people) have practiced social engineering for years, and so have debt collectors, bounty hunters, private investigators, and journalists. Phishing does this via email or malicious websites.

²⁷ A Trojan Horse is malicious program masquerading as a safe and useful one.

²⁸ A vulnerability involved in the Target breach, for example. See Brian Krebs, *Inside Target Corp., Days After 2013 Breach*, KREBS ON SECURITY (Sept. 21, 2015), <https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/>.

²⁹ Target did not encrypt credit card numbers on their way out of the POS machine, instead of at the point of swipe. *Id.*

³⁰ The 80 million records stolen from Anthem in 2015 were stored unencrypted and hence readable by the thieves. See, e.g., Lance Whitney, *Anthem’s Stolen Customer Data Not Encrypted*, CNET (Feb. 6, 2015, 10:06 AM), <https://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/>.

³¹ See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

breach, which was particularly well studied, we know that there was quite a significant number of vulnerabilities that together enabled a breach of that magnitude.³² It seems likely that, for many of the massive data breaches, a combination of several different vulnerabilities enabled the breach.

Some network vulnerabilities are certainly software vulnerabilities since software (both mass market and non-mass market) is involved in running a network. Since human beings use networks, human vulnerabilities are also common. But not all network vulnerabilities are software or human ones. From now on, we will use “network vulnerabilities” to refer to non-software, non-human vulnerabilities in networks. These vulnerabilities are the ones whose remediation requires information that is not currently available.

To characterize network vulnerabilities, we offer a brief high-level sketch of how network security works. It works much like security at Chicago’s United Center—the sports arena where the Bulls play basketball and the Blackhawks play hockey. If you oversaw security there, you would locate the doors and windows, put locks on all those doors and windows, lock the ones you do not need open, and post guards at the rest to check credentials like tickets, press passes, etc. You would also put guards inside to monitor behavior. Computer and network security is the same. You lock doors and windows,³³ post “credential-checking guards” by verifying authorization,³⁴ and deploy “behavior-monitoring guards,” ranging from home computer antivirus programs to multimillion-dollar systems defending corporate networks.³⁵

Likewise, competent network administrators know how to reduce network vulnerabilities.³⁶ Notice that we wrote “reduce,” not “eliminate.” In a large organization, both the routers and internal structure of the network can be quite complex, and the more complex the network, the more likely a misjudgment that creates a vulnerability. In addition, hackers “are well aware of the details of network . . . security mechanisms, and are developing increasingly sophisticated and effective methods for subverting them.”³⁷ Thus, if businesses were meeting the risk management goal, we would ex-

³² MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER, S. COMM. ON COMMERCE, SCIENCE, AND TRANSP., A “KILL CHAIN” ANALYSIS OF THE 2013 TARGET DATA BREACH (2014), https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf.

³³ Examples include promptly applying patches, using reasonably up-to-date operating systems, and various uses of encryption.

³⁴ Examples include passwords, more complex multi-factor identification, access control, firewalls, and both black and white listing.

³⁵ Examples include intrusion detection and protection systems, some forms of malware detection, and various forms of traffic monitoring.

³⁶ See STALLINGS, NETWORK SECURITY ESSENTIALS, *supra* note 7.

³⁷ Archit Gupta et al., *An Empirical Study of Malware Evolution* 1, 1 (2009 First International Communication Systems And Networks Workshops, 2009).

pect to see a few network vulnerabilities. However, in practice, based on the past decade's record of breaches, there are *lots* of network vulnerabilities.

So why, in regard to network vulnerabilities, do businesses typically fail to meet the business risk management goal? One reason is that corporate culture has struggled to incorporate that goal in its business planning.³⁸ Lack of risk management expertise is another problem.³⁹ We assume businesses will eventually solve those problems. Doing so will not, however, eliminate a fundamental problem: the lack of information necessary for adequate risk assessment.

C. *The Lack of Information*

To adequately approximate the business risk management goal, a business has to calculate the expected losses from a data breach over some appropriate period of time. The expected cost of a data breach is the estimated actual cost of the breach if it occurs multiplied by the probability of its occurrence. If a business bases this calculation on accurate information about probabilities and costs, pursuing the business risk management goal is a profit maximizing strategy. The more inaccurate the information, the worse the business's strategy; it will either spend too much or too little.

Unfortunately, there is general agreement that businesses lack sufficiently accurate information about probabilities and costs. A recent World Economic Forum report paints an accurate, if disturbing, picture of the lack of relevant data:

There are numerous cyber threats plaguing global organizations. Global data is expanding at exponential rates in terms of volume, velocity, variety and complexity. Commercial and personal data are increasingly migrating to global, interconnected technology platforms. The systems that depend upon this data increasingly manage key infrastructure. As access to data and systems increases via the rapidly evolving, interconnected digital ecosystem, the scale and types of risks from cyber threats expands proportionately.

Unknowns concerning the scale and impact of cyber threats, as well as relative levels of vulnerability, threatens paralysis. Lacking accepted benchmarks, large organizations struggle to structure cyber resilience decisions and investments. Organizations lack common measures to quantify cyber threats, curtailing the ability to make clear strategic decisions concerning optimal access and investment levels.

³⁸ See, e.g., Marianne Davis, *Underinvesting in Cybersecurity: How Do You Know How Much Security Is Enough?*, SYMANTEC (Aug. 15, 2014), <http://www.symantec.com/connect/blogs/underinvesting-cybersecurity-how-do-you-know-how-much-security-enough>.

³⁹ DOUGLAS W. HUBBARD ET AL., HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK 11–15 (2016).

Due to this state of uncertainty, a pervasive concern over growing cyber risks curtails technical and economic development on a global scale. Lacking proper guidance, businesses are increasingly delaying the adoption of technological innovations due to inadequate understandings of required countermeasures. A tragedy of the commons scenario is emerging surrounding proliferating digital access in an unstable ecosystem, which lacks concerted controls and safeguards. A vicious circle results: uncertainty regarding proper levels of preparedness leads to forestalled investments in safeguards as interconnection expands exponentially.⁴⁰

The report identifies two sources of uncertainty. The first is that the magnitude of the losses is not sufficiently well known: there are “[u]nknowns concerning the scale and impact of cyber threats.” The second is that the probability of a loss is not sufficiently well known: there are “[u]nknowns concerning . . . relative levels of vulnerability.” This puts a significant roadblock in the way of pursuing the business risk management goal.

The same point holds for *consumer* risk management, to which we now turn.

II. DEFENDING CONSUMERS

Risk management, whether business or consumer, requires reliable information—ideally, highly accurate information—about both the magnitude of the loss and the probability of its occurrence. For consumer risk management, the relevant magnitudes and probabilities are the magnitudes and probabilities of *consumer* losses. Neither is sufficiently well known. There have been far fewer studies of consumer losses, and, if it is problematic to accurately correlate the cost and probability of business losses with types of data breach, it is all the more difficult to do so in the case of consumer losses, where the relevant data is less available.

In the consumer context, the lack of information has consequences for the effectiveness of making businesses legally liable for consumer losses. Before turning to that issue, we briefly address the prior question of whether businesses should be liable for those losses.

⁴⁰ WORLD ECON. FORUM, PARTNERING FOR CYBER RESILIENCE TOWARDS THE QUANTIFICATION OF CYBER THREATS 9 (2015), http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf. Others make the same points: “It has also long been known that we simply do not have good statistics on online crime, attacks and vulnerabilities. Companies are hesitant to discuss their weaknesses with competitors even though a coordinated view of attacks could allow faster mitigation to everyone’s benefit. In the USA, this problem has been tackled by information-sharing associations, security-breach disclosure laws and vulnerability markets.” Ross Anderson et al., *Security Economics and European Policy* 3 (2008), <http://www.cl.cam.ac.uk/~rja14/Papers/enisa-short.pdf>.

A. *The Landlord/Tenant Analogy*

There is a strong argument that businesses should bear a considerable part of the defensive burden. Consider an analogy with landlords and tenants. The “landlords” are the various kinds of businesses that store consumer data online.⁴¹ Call them collectively *data holders*. “Tenants” divide into the data that resides with the data holder and the consumer subjects of that data. What makes the analogy apt is that unauthorized access to the data can harm the subjects. The argument is that just as landlords can be liable for harm to tenants from unauthorized access to the landlords’ buildings, so data holders should be liable for harm caused to consumers by unauthorized access to the data they store. To see the argument, consider the landlord/tenant case, *Kline v. 1500 Massachusetts Avenue Apartment Corporation*.⁴² Kline was assaulted in the common areas of the apartment building in which she lived.⁴³ She sued for negligence alleging that the building owner unreasonably failed to provide adequate security.⁴⁴ The court agreed:

The landlord is no insurer of his tenants' safety, but he certainly is no bystander. And where, as here, the landlord has notice of repeated criminal assaults and robberies, has notice that these crimes occurred in the portion of the premises exclusively within his control, has every reason to expect like crimes to happen again, and has the exclusive power to take preventive action, it does not seem unfair to place upon the landlord a duty to take those steps which are within his power to minimize the predictable risk to his tenants.

....

As between tenant and landlord, the landlord is the only one in the position to take the necessary acts of protection required. He is not an insurer, but he is obligated to minimize the risk to his tenants. Not only as between landlord and tenant is the landlord best equipped to guard against the predictable risk of intruders, but even as between landlord and the police power of government, the landlord is in the best position to take the necessary protective measures. Municipal police cannot patrol the entryways and the hallways, the garages and the basements of private multiple unit apartment dwellings. They are neither equipped, manned, nor empowered to do so. In the area of the predictable risk which materialized in this case, only the landlord could have taken measures which might have prevented the injuries suffered by appellant.⁴⁵

The court held that the landlord was required to take reasonable steps to defend tenants in common areas from harm from unauthorized access to

⁴¹ Businesses range from resource- and expertise-rich corporations to mom-and-pop retailers. There is a pressing question of how small and medium sized businesses are to meet the risk management goals we suggest here.

⁴² *Kline v. 1500 Massachusetts Ave. Apartment Corp.*, 439 F.2d 477 (D.C. Cir. 1970).

⁴³ *Id.* at 478.

⁴⁴ *Id.* at 489.

⁴⁵ *Id.* at 481, 484.

those areas.⁴⁶ Advances in technology have resulted in a new type of “landlord”—data holders. Like traditional landlords, they are typically in the best position to take steps to prevent the harm to data subjects that may follow a data breach.

So why not require data holders to take reasonable steps to prevent harm to the data subjects? We find that rationale to do so compelling, and, indeed, to an extent, the law already does so through common law negligence⁴⁷ and through various statutory requirements.⁴⁸ We will not discuss the exact form the reasonableness requirement should take. Our point is that unless the necessary risk management information is available, a reasonableness requirement will be ineffective.

B. *Lack of Data Means Lack of an Effective Legal Incentive*

To see why, consider an analogy. Suppose you are a teacher who would like students to write something to engage in adequate explanation and reflection. To achieve this goal, you tell them they must write a paper with enough pages to get a passing grade, but you do not tell them how many pages are enough. That would not only be unfair, it would also fail to create the right incentive for sufficient explanation and reflection. Some would write too little, expending less time and effort than they should, some would write too much, expending more time and effort than they should. Network defense is similar. Some businesses will invest too little in defense, some, too much.

Some may object that this argument looks only at the short-term consequences of imposing liability in the absence of relevant information about probabilities in costs. Why not impose liability to give businesses an incentive to develop ways to obtain the information they now lack? The classic torts case of *The T. J. Hooper*⁴⁹ is a good example, even though it involved providing an incentive to adopt technology that already existed, not providing an incentive to create information gathering practices that do not.

The tugboats the *Montrose* and the *T. J. Hooper* encountered a gale while towing barges up the Atlantic coast, and the tugs and the barges

⁴⁶ See *id.* at 487.

⁴⁷ At least in theory. The application of negligence is limited by the foreseeability requirement (see, e.g., *Guin v. Brazos Higher Education Service Corporation, Inc.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483, (D. Minn. Feb. 7, 2006) and the economic harm rule (see, e.g., *Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006)).

⁴⁸ See, e.g., HIPAA Security Rule 45 C.F.R. § 164.308(A)(1), and the Gramm-Leach Bliley Safeguards Rule, 16 C.F.R. § 314.3. For an excellent discussion of the Federal Trade Commission's approach to security, see CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

⁴⁹ The *TJ Hooper*, 60 F.2d 737 (2d. Cir. 1932).

sank.⁵⁰ The tugs did not have shortwave radios.⁵¹ Had they been so equipped, they would have received reports of the storm and put in at the Delaware breakwater to ride the storm out in safety.⁵² Shortwave radios, however, were new technology, and the industry standard was for tugs *not* to have one.⁵³ The court nonetheless held that it was unreasonable not to equip the tug with a radio as a precaution against losses from storms.⁵⁴

But notice that the risk management calculations are easy. It is obvious that the expected loss exceeds the cost of the radio. Owners know that the losses, when they do occur, can be huge, and they know that, while the occurrence of violent storms is difficult to predict, their occurrence from time to time is certain. So, tugboat owners should realize that they should buy a radio.

So why not impose liability for consumer losses from a data breach to give businesses an incentive to develop and implement effective information gathering practices? The incentive is unlikely to be effective. Contrasts with *The T. J. Hooper* show why. To begin with, tug boat owners could unilaterally buy shortwave radios, but businesses cannot unilaterally collect enough information. To figure the relevant probabilities and costs for a wide range of possible data breaches, a business needs information about the types of data breaches and associated losses that occur across a wide range of businesses. Determining probabilities and costs will require aggregating that information.

III. BETTER DEFENSE WITHOUT BETTER DATA?

Lack of sufficient information about relevant probabilities and costs does not mean it is impossible for businesses to improve their data security. We consider three possibilities: reliance on expert opinion, outsourcing, and compliance with data breach notification statutes. Each option, however, falls far short of approximating the business and consumer risk management goals.

⁵⁰ *Id.* at 737.

⁵¹ *Id.*

⁵² *Id.*

⁵³ *See id.* at 740.

⁵⁴ *See id.*

A. *Expert Opinion*

Lacking sufficient information to accurately determine probabilities and costs,⁵⁵ businesses can turn to educated guesses—that is, to well-informed expert opinion. As one predictive analytics practitioner noted:

Where very little data is available, it's not possible to use standard mathematics or statistical techniques, but what you can do is create models based on expert opinion. These won't be as good as a statistical model built on a much larger sample, but these types of models can often provide a reasonable level of predictive accuracy.⁵⁶

Relying on expert opinion is reasonable given the current lack of information. But, relying merely on expert opinion is still not a reliable guide to meeting either risk management goal. Expert opinion may still over- or underestimate probabilities and costs, and in such cases a business will spend less or more than required to meet the goal.

B. *Outsourcing*

Outsourcing security recommends itself as at least a partial solution to the lack of information problem. One necessary step toward curing the lack of information is aggregating relevant information from a wide variety of businesses. Outsourcing security will help with that task by concentrating the information from several businesses in a single place. Outsourcing also makes good financial sense. As security and privacy expert Bruce Schneier noted:

A company can get the security expertise it needs much more cheaply by hiring someone else to provide it. Take monitoring, for example. The key to successful security monitoring is vigilance: attacks can happen at any time of the day, any day of the year. While it is possible for companies to build detection and response services for their own networks, it's rarely cost-effective. Staffing for security expertise 24 hours a day, 365 days a year, requires five full-time employees—more when you include supervisors and backup personnel with specialized skills. Even if an organization could find the budget for all of these people, it would be very difficult to hire them in today's job market. Retaining them would be even harder. Security monitoring is inherently erratic: six weeks of boredom followed by eight hours of panic, then seven weeks of boredom followed by six hours of panic. Attacks against

⁵⁵ In the case of the frequency interpretation of probability, a determination is accurate if closely approximates the actual frequency. For the belief interpretation, a determination is accurate to the extent it requires little or no revision in the light of future information.

⁵⁶ STEVEN FINLAY, PREDICTIVE ANALYTICS, DATA MINING AND BIG DATA: MYTHS, MISCONCEPTIONS AND METHODS 232 (2014).

Security outsourcing companies like AllClearID, BayDynamics, Healthguard Cyber Risk Management, and FireEye provide reasonable security options, especially for small and medium-sized businesses that may not be able to afford a significant investment in information security. Indeed, because basic outsourcing services are sufficiently inexpensive, they may be the twenty-first century equivalent of *The T. J. Hooper* shortwave radio. One may well see legal liability imposed for not using them.

Outsourcing is an attractive and important development; however, as currently practiced, it relies on models built using expert opinions, so it does not lead to an adequate approximation of either risk management goals. There are also privacy concerns. Businesses outsourcing security run their incoming data through the outsourcer. The outsourcer's access to the information raises privacy concerns, and some outsourcers do indeed analyze this data for advertising purposes.

C. *Data Breach Notification Laws*

Data breach notification laws may seem like an attractive option that both forces the disclosure of information about breaches without the privacy concerns of outsourcing and improves security, so its proponents claim. As Bruce Schneier notes:

There are three reasons for breach notification laws. One, it's common politeness that when you lose something of someone else's, you tell him. The prevailing corporate attitude before the law—"They won't notice, and if they do notice they won't know it's us, so we are better off keeping quiet about the whole thing"—is just wrong. Two, it provides statistics to security researchers as to how pervasive the problem really is. And three, it forces companies to improve their security.⁵⁸

We focus on the second and third reasons, beginning with the third. The laws certainly do lead businesses to increase security. The reason is that publicizing data breaches can impose significant costs on businesses,⁵⁹ and the threat of such losses has led businesses to increase online security.⁶⁰

Does the increase yield a more effective pursuit of the goal of consumer risk management? We have found little relevant evidence, other than

⁵⁷ Bruce Schneier, *The Case for Outsourcing Security*, SCHNEIER ON SECURITY (2002), https://www.schneier.com/essays/archives/2002/01/the_case_for_outsour.html.

⁵⁸ Bruce Schneier, *State Data Breach Notification Laws: Have They Helped?* SCHNEIER ON SECURITY (2009), https://www.schneier.com/essays/archives/2009/01/state_data_breach_no.html.

⁵⁹ *Cost of Data Breach Study*, *supra* note 2, at 19.

⁶⁰ *Cost of Data Breach Study*, *supra* note 2, at 15.

a study focusing on identity theft.⁶¹ There is some evidence that the laws reduce identity theft.⁶² The identity theft study correlates the existence of data breach notification laws with reductions in identity theft.⁶³ One cannot simply infer, however, that an increase in security is responsible for the reduction. Reductions in identity theft may result from a variety of factors other than increased security.⁶⁴ Furthermore, even if data breach laws do trigger increases in security that reduce identity theft, that still falls short of showing that those laws decrease overall consumer risk to the point where the consumer risk management goal is attained. The reason is that the harm from unauthorized access reaches far beyond identity theft. It includes harm from ransomware, denial of services attacks, botnets engaged in fraud and other illegal activities, and viruses.⁶⁵ The available evidence is thus inconclusive at best.

There is, moreover, a general reason to doubt that data breach notification requirements get us to the consumer risk management goal. It emerges from considering the costs of compliance with notification requirements. Those costs include: forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors, notification costs, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions, and lost business.⁶⁶ Data breach notification laws create an incentive to avoid *those* costs. It would be surprising if avoiding those *business* costs were strongly correlated with improved *consumer* risk management.

Indeed, there is some reason to think such a correlation is unlikely. The reason is that the laws define the type of event a business must report.⁶⁷ They thus create an incentive to reduce *reportable* data breaches. They do not create an incentive to improve security in regard to problems that do not manifest themselves as reportable data breaches. As professor David Thaw

⁶¹ David Thaw's work is an important exception. See David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE NOVO 163 (2015) (arguing that "an affirmative presumption of notification is superior from a cybersecurity perspective. Such a presumption avoids disincentivizing thorough cybersecurity investigations, which are one of the most important tools in protecting consumers against future data breaches and securing existing information systems.")

⁶² *Id.* at 161.

⁶³ *Id.*

⁶⁴ Richard J. Sullivan & Jesse Leigh Maniff, *Data Breach Notification Laws*, FED. RESERVE BANK OF KANSAS CITY, <https://www.kansascityfed.org/~media/files/publicat/econrev/econrevarchive/2016/1q16sullivanmaniff.pdf>.

⁶⁵ DETICA, *supra* note 4, at 2.

⁶⁶ *Cost of Data Brach Study*, *supra* note 2, at 3.

⁶⁷ CENT.S FOR MEDICARE & MEDICAID SERV.S, *CMS Information Security and Privacy Overview*, <https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/informationsecurity/> (last modified Apr. 27, 2018).

notes, specific statutory regulations like data breach notifications laws can drive

perhaps-otherwise-sufficient security budgets toward specific compliance objectives, such as encryption. This, in turn, reduces the available resources for other security activities and forces CISOs to focus on meeting minimum compliance objectives rather than prioritizing the greatest threats they feel their organization face[s]. With an abundance of low-hanging fruit available to regulators—even if likely through malfeasance, not misfeasance—the bar is set extremely low. Thus, regulators are faced with an "industry standard" set perhaps below their optimal level. As long as low-hanging fruit remains available to regulators, CISOs will not be able to justify requests for new resources on the grounds that peer organizations with comparable policies have been subject to enforcement action. Nor will they be able to justify requests based on the regulations themselves, as "reasonable" lacks an operational definition any higher than the low hanging fruit provided by cases [involving obvious and egregious security weaknesses] such as *B.J.'s Wholesale Club*, *T.J. Maxx Cos.*, and *Twitter*. And so the cycle continues.⁶⁸

Similar worries arise for the role of data breach notification laws in forcing businesses to divulge information about data breaches. They certainly do that. But the information businesses provide is only information about reportable data breaches. Data breach notification laws do not create an incentive to report information about data breaches generally.

IV. MANDATORY ANONYMOUS REPORTING

To estimate the probability of a data breach, we need information about the occurrence of data breaches across a wide range of businesses. The costs of a data breach divide into the costs to businesses and the costs to consumers. To aggregate information about the occurrence of data breaches and their costs to *businesses*, we suggest obtaining that information through *mandatory* collection in a central depository and through the sharing of an *anonymous* summary of the data to all of the mandatory reporters. The data would allow the depository to provide high quality data to the business world about the actual prevalence and cost of breaches in practice today.⁶⁹ Mandatory sharing has at least two advantages over voluntary sharing. If sharing is voluntary, businesses will weigh the benefits of

⁶⁸ David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. UNIV. L. REV. 287, 368-69 (2014).

⁶⁹ Some worry that the data may have limited predictive value. See Annmarie Geddes Baribeau, *Cyber Insurance: The Actuarial Conundrum*, INSUR. COMMUN. 33, 37-38 (2015) (providing, "[W]hile actuaries do need as much historical data as they can get, past data is not always indicative of future events or their costs. 'The challenge is much greater than not having enough historical data . . . Because cyber risk is both growing and rapidly evolving, information about the past may be of limited predictive value.'"). To some extent, the risk that one's data is not representative is inherent in all risk management. Where cyber risk changes rapidly, companies would be well advised to base their predictions on a smaller, more recent sample rather than a larger, but necessarily less recent sample.

information sharing with the risks and costs of doing so, and they may decide that the benefits are insufficient. In particular, at the beginning of a voluntary program, the initially small pool of information means limited benefits, so businesses may be unwilling to participate until enough others do. It may be possible to overcome these problems, but we put them aside. Our concern is to defend mandatory sharing as an acceptable option.

There are at least three existing models in the broad ballpark of what we have in mind. One is the 2015 Cybersecurity Information Sharing Act (CISA), which is voluntary, but covers quite similar information.⁷⁰ The second is the mandatory reporting of certain electrical outages to the Department of Energy (DOE).⁷¹ Finally, there is the required, completely confidential reporting of network outages to the FCC under the Network Outage Reporting System (NORS).⁷² Each of these three is informative, but not one is a perfect match. CISA is voluntary.⁷³ The DOE reporting covers a much smaller number of incidents than any estimates of the current number of computer security incidents; for example, the public summary of electrical outage events from January through July 2017 shows only 91 total reported events.⁷⁴ The data from NORS does not become public nor, as far as we know, is it ever shared with the cable, satellite, telephone, etc. companies that provide the data to the FCC; the FCC says, “Given the sensitive nature of this data to both national security and commercial competitiveness, the outage data is presumed to be confidential.”⁷⁵

To aggregate information about the *consumer* cost of data breaches, we do *not* propose any sort of mandatory reporting by consumers to the government. It would raise significant privacy issues to require consumers to report the type of data involved in a breach, the storage location of the data, and the type and extent of the losses sustained. We propose instead government-initiated or government-funded research, which focuses on consumers who consent to provide their information. The approach is far from unproblematic, but we put those issues aside. We focus primarily on mandatory reporting by businesses.

⁷⁰ CYBER SECURITY INFORMATION SHARING ACT OF 2015, 6 U.S.C. § 148.

⁷¹ 15 U.S.C. § 772 mandates the sharing of the information. See Emily Fisher, Joseph H. Eto & Kristina Hamachi LaCommare, *Understanding Bulk Power Reliability: The Importance of Good Data and a Critical Review of Existing Sources* 2159–2168 (2012 45th HI Int’l Conf. on Sys. Sci., 2012), <http://ieeexplore.ieee.org/abstract/document/6149274/>.

⁷² FED. COMM’NS. COMM’N., *Network Outage Reporting System (NORS)*, <https://www.fcc.gov/network-outage-reporting-system-nors> (last viewed Dec. 4, 2018).

⁷³ CYBER SECURITY INFORMATION SHARING ACT, 6 U.S.C. § 148.

⁷⁴ DEPARTMENT OF ENERGY, *Electric Disturbance Events (OE-417) Annual Summaries*, https://www.oe.netl.doe.gov/OE417_annual_summary.aspx (last visited Dec. 4, 2018).

⁷⁵ FED. COMM’NS. COMM’N., *supra* note 72.

A. *Sketch of Our Proposal for Reporting*

We propose a reporting regime for computer security incidents for organizations that are closest to the DOE electrical outage reporting, or more specifically, to the first part of the DOE's mandatory two-part reporting form, OE-417.⁷⁶ That form has two parts, Schedules 1 and 2; the first part is highly structured, consisting of checkboxes, and constrained, very short answer questions, such as "estimate number of customers affected," and fits on two pages.⁷⁷ Schedule 1 is made public.⁷⁸ Schedule 2, which asks for a narrative description, is not made public.⁷⁹

Similarly, we envision a mandatory report that would consist of checkboxes and very short answer questions asking for the size, type, and estimated costs of a breach, along with several attributes about the organization attacked and its defenses. As mentioned, the DOE makes the Schedule 1 information from every reported electrical outage incident public.⁸⁰ We would do the same, but redact the name of the organization and any geographic information. We would also round numerical reports, making them at least modestly more difficult to associate with particular incidents. The goal is not to anonymize all reports, but rather to attempt to anonymize many of the reports of smaller incidents.⁸¹ Because the major incidents are often widely reported news events and may also be subject to mandatory public disclosure, there is no point in trying to anonymize them.

B. *Benefits of the Proposed Reporting*

The information gathered and reported, together with an estimate of the number of organizations required to report, will give both researchers and organizations themselves the data needed to make reasonably accurate estimates of the probability of a security incident, and more specifically, the probability of a security incident of a specific cost. This is precisely the information that we have argued is needed but is currently missing. It

⁷⁶ U.S. DEP'T OF ENERGY, OE-417 ELECTRIC EMERGENCY AND DISTURBANCE REPORT, https://www.oe.netl.doe.gov/docs/OE417_Form_05312021.pdf (last visited Dec. 3, 2018).

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ We write "attempt to anonymize" rather than "anonymize" because of the frequent successes of computer scientists in deanonymizing supposedly anonymized datasets over the past decade or two. See, e.g., A. Narayanan & V. Shmatikov, *De-anonymizing Social Networks* 173–187 (PROC. OF IEEE SYMP. ON SECURITY AND PRIVACY 2009); Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets* 111–125 (PROC. OF IEEE SYMP. ON SECURITY AND PRIVACY 2008); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

makes sense for the federal government to collect this data nationwide, but that is not absolutely necessary. If just a handful of states, or even one large enough state with enough business activity were to gather and report this information, then that would probably suffice. Estimates of breach probabilities based on, say, only California or only Texas would not be quite as accurate as those based on the nation as a whole, but they should still be quite good.

The collection we have in mind should be able to be done at quite a low cost for both the reporting companies and for whatever government agency collects and publishes it. There is no reason a report shouldn't fit on a two-page form, just like Schedule 1 of OE-417.

C. *Privacy Concerns?*

Prior to its passage, privacy advocates “asked Congress to kill or reform the Cybersecurity Information Sharing Act, a bill that they [said hid] new government surveillance mechanisms in the guise of security protections.”⁸² The issue was that the shared information in CISA could include detailed information about various consumers’ data or online behavior if it was relevant to a breach. It is difficult to see how our proposal, for short reporting of the size and nature of a breach and an organization’s defenses, could become a surveillance system in the guise of security protection. We envision businesses reporting only the size, type, and approximate cost to the business of a breach along with several relevant attributes of the business and its defenses. With a little information on which organizations are required to report, this would allow businesses and other organizations to calculate expected business losses. It is difficult to see how sharing and disclosing such information threatens privacy.

V. CONCLUSION

Business and consumer information sharing can provide the data necessary to adequately approximate the business and consumer risk management goals. This would improve defenses against data breaches by reducing network vulnerabilities. It would do so on two conditions. First, businesses incorporate the risk management goals into their business planning.⁸³ Second, businesses have sufficient information about data breach losses, and they face liability to some appropriate extent for failing to meet the

⁸² Michael Reynolds, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015, 5:30 PM), <https://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/>.

⁸³ See generally *supra* notes 14–15 and accompanying text.

consumer risk management goal. Even then, information sharing remains a partial solution to the problem of improving data breach defenses. One must also reduce software and human vulnerabilities. Information sharing is nonetheless an essential step in the right direction.