Are Firms and Consumers Investing Enough in Data Security?

Sasha Romanosky,
sromanos@rand.org
RAND Corporation

Do firms and consumers take enough care to protect personal information? Many consumer advocates and security and privacy professionals have concluded that companies are not spending enough on IT security. Their assessments are buttressed by the numerous reported cyber incidents and data spills over the past decade. Clearly, these security breaches, privacy intrusions, and software vulnerabilities show that companies are not spending enough to protect consumers' data and produce safe applications. But there are two problems with this conventional wisdom. First, it ignores the consumer in the model of optimal data security. And second, it wrongly assumes that the right level of security investment would eliminate data breaches altogether.

This white paper helps correct the discussion on both counts.[1]

I. The Consumer as Data Security Investor

Discussions of data security implicitly assume that consumers cannot, or should not, take measures to protect their own data and computers. Certainly, there are many circumstances when individuals have little or no control over the fate of their personal information (e.g. hack of a firm's computers that had collected personal data without consent, causing identity theft). However, there are also many situations where individuals have the option to take greater measures to protect their information, such as using better, and more unique passwords with password manager software, sharing less information online (and offline), and ensuring their devices are regularly patched.

Consumers, just like companies, are self-interested. We make decisions to maximize our welfare, and we shirk responsibilities when our behavior poses no consequence to us (as when merchants bear the risks from identity theft rather than the card holder.) Therefore, when considering policy interventions for the firms, it is also reasonable to consider whether policymakers should induce individuals to take more precautions to protect their digital assets.

[1] A related version of this paper appeared in "Building Common Approaches for Cybersecurity and Privacy in a Globalized World, Transatlantic Conference, NYU Center for Cybersecurity & Humboldt Institute for Internet and Society," October, 2018.

And so any discussion of how to induce companies[2] to invest in security measures should be accompanied with a similar analysis of consumer behavior to ensure that both parties take appropriate security and privacy precautions.

II. Optimally Imperfect Security

My second concern is that each data breach is treated as per se evidence of inadequate security. The presumption that companies do not invest enough in security often implicitly assumes that if firms *do* invest an ideal amount, there would be no data breaches or security incidents at all. "Appropriate" security is assumed to be absolute security. But of course, perfect security is neither practical nor efficient. If instead what is being sought is for companies to invest in a *reasonable* level of precaution, then this would suggest that firms take all appropriate, cost-effective steps. These steps are unlikely to remove every last vulnerability.

Lawmakers who are accustomed to using cost-benefit analysis as the basis for establishing reasonable care will be familiar with these ideas. Just like with accidents, it is true that increased spending on precautions can reduce security incidents. But that additional (marginal) cost of investment may be larger than the (marginal) benefit from that investment. And so, if efficiency is the guiding light, we must acknowledge a tolerance for, and be accepting of, data breaches.

Moreover, the data breaches that occur today do not necessarily prove that companies (or individuals) have failed to use an efficient amount of protection. To the contrary, an absence of security breaches would suggest that firms are *over-investing* in security. To date, the policy conversation about data security has not established a baseline level of acceptable risk. There has been little effort to test the null hypothesis that firms are already investing in an appropriate level of care, and thus little reason to reject it. The problem may not be that firms are under-investing, but rather that our current capabilities of security risk assessment are unable to determine whether they have or not.

Thus, before we answer the question "how should we get companies to invest more?," we must first ask, "*should* we get companies to invest more?"

III. Ex Ante vs Ex Post Regulation

The goal of the policy maker should be to induce firms and consumers to *optimize* -- not minimize -- security incidents. That is, it should seek to balance the incremental cost of a security measure with its incremental benefit, in order to achieve the most efficient level of care.

The field of law and economics is very informative as way to understand alternative policy interventions, and when they are most and least effective.[3] These interventions are often framed

[2] Note that in discussing "companies" or "firms," we are considering a wider frame than just the specific entities that hold personal consumer data. Indeed, there are many organizations involved in many different kinds of transactions and data exchange agreements, such as the firm that authenticates a credit card or loan application, social media sites, content providers, advertisers, data aggregators, etc. For simplicity, we consider any firm that acquires, stores, processes, or manages personal information.

as driving behavior either before an accident has occurred (*ex ante*), or afterward (*ex post*). Ex post liability, for example, works best when the source of a particular injury is known, and the harms relate to personal injury or property damage – that is, physical and tangible harms. In the context of online data breaches and electronic identity theft, however, the current judicial system is still struggling to adequately address these harms precisely because these two assumptions are challenged.[4]
Effectively, data breaches and resulting identity theft can be characterized as a bilateral care accident model – where two parties are meant to take precautions to reduce harm. For example, consider a car and pedestrian. They both need to take precautions to avoid an accident. Tort law tries to ensure appropriate levels of precaution by both parties by setting a level of due care on the injurer (i.e. cars shouldn't hit pedestrians), yet also applying contributory or comparative negligence standards for the victim – effectively saying that pedestrians also need to take some measure of precaution to avoid being hit, and thereby preventing moral hazard.

Ex ante regulation (aka compliance) works well when the source of an injury is unknown, and the harms are either so catastrophic that society could not tolerate them (e.g. nuclear accidents), or where they are miniscule, but distributed across many people (e.g. incremental environmental damage). Ex ante regulation is also preferred in situations where it is easier to monitor ex ante compliance than it is to detect and source an injury ex post. This is usually the case when there is considerable delay between a breach of reasonable care and the actual harm, such as with data breaches and identity theft. Ex ante interventions are also most useful when the state (or regulator) has better information about harms than either the firms, or the victims, and when the level of care is unobservable, such as is often the case with cyber security.

However, ex ante interventions require regulators to establish a clear standard of care. This is a straightforward process when an industry's inputs are strongly associated with harmful outputs. For example, if we know which security precautions are best able to prevent harms, we can recommend or mandate those precautions, and then encourage or enforce their adoption. Unfortunately, the security field has failed to identify which security controls work best, and especially which security controls work better than others at preventing loss.

The weaknesses in our evidence base are discussed in more detail next.

IV. Cybersecurity as a Risk Management Problem

As public awareness and appreciation for cybersecurity have evolved, firms have started to manage cyber risk like any other serious business threat. Cybersecurity now receives boardroom level attention.[5] But even as cyber risk has demanded an increasing share of attention, cybersecurity is still just one risk among many that firms must manage. For instance, they must

---

[3] Shavell, S. (2014) Foundations of Economic Analysis of Law. Belknap Press.
[4] Romanosky, S., Hoffman, D., and Acquisti, A. (2014). Empirical Analysis of Data Breach Litigation. Journal of Empirical Legal Studies, 11(1), 74–104.
[5] See World Economic Forum's 2018 report citing cyber risks as the second most critical risk, http://reports.weforum.org/global-risks-2018/executive-summary/ and Travelers Risk index 2018 which cites cyber as the 2nd gravest overall risk https://www.travelers.com/resources/risk-index/2018-cyber-infographic. Last accessed January 7, 2019.

address legal and regulatory risks arising from criminal, civil, and government agency enforcement actions. They must manage tax and other financial risks related to short and long-term investments and cash flow, and they must manage political, workforce and supply chain risks, as well as other operational, and R&D risks.

If we believe that firms should address cyber as a risk management problem, we must recognize firms' competing risks and their constrained resources. They simply cannot eliminate all risks, and so they must prioritize. Therefore, by advocating for managing cyber risk this way, we must accept that if, after a thoughtful assessment, cyber risk is determined to be less grave than other potential problems, it will be appropriately deprioritized.

In two recent studies, researchers examined the cost of breaches, and consumer sentiments in response to data breach notifications. [6] Two important insights emerged. First, losses due to cyber incidents make up less than 1% of a firm's revenue. Relative to other forms of fraud, waste and abuse as measured in other industries, cyber losses are much smaller. Second, from a survey of individuals who had received breach notification letters, people seemed relatively comfortable with firm responses (transparent notices, and offers of free credit monitoring). Together, these results suggest that cyber incidents do not impose as much harm for either firms or consumers as we might be led to believe. And so, if true, this provides some explanation for why some firms are not investing in higher levels of data security. Moreover, it may explain why consumers, as well, are not taking more precautions than we often criticize them for. If they simply aren't incurring any penalties from data breaches, then why bother with better password management, or applying security patches to their devices?

Now, it may be the case that cyber risks are not correctly assessed or effectively presented to corporate executives (or to their consumers) in a way that accurately reflects the potential losses for all stakeholders. Security professionals and researchers have not been able to measure and communicate cyber risk adequately. Collectively, we cannot answer basic questions like: am I more secure now relative to last year? Or how much should I invest in cyber security this year?

There are many cyber security risk frameworks (e.g. FAIR, OCTAVE, NIST[7]), but none of them are able to answer these questions because they all rely on subjective assessments, best practices, or are influenced by data limitations, behavioral biases, and modeling assumptions – anything other than empirical evidence.

The best that the industry is able to do is conjure up and track handfuls of metrics that we think are most correlated with better security posture and ultimately our ability to withstand an attack[8].

---

[6] Romanosky, S. (2016). Cost and Consequences of Cyber Incidents, Journal of Cybersecurity, 2(2), 121-135; Ablon, L., Heaton, P., Lavery, D., Romanosky, S., Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information, RAND Corporation, RR-1187-ICJ, 2016.

[7] See https://insights.sei.cmu.edu/insider-threat/2018/06/octave-forte-and-fair-connect-cyber-risk-practitioners-with-the-boardroom.html and https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework. Last accessed January 7, 2019.

[8] Jaquith, A. (2007) Security Metrics: Replacing Fear, Uncertainty, and Doubt 1st Edition, Addison-Wesley Press.

Security metrics afford us a tangible way to demonstrate progress, for example, showing the number of vulnerabilities identified and remediated each month, or the number of malware infections per quarter. Unfortunately, we have little proof that any one, or group of metrics, is truly effective. Likely some of them are, of course, but we just don't know which, or by how much.

V. What is the Role of Cyber Insurance?

It is tempting to turn to the insurance industry for answers. In other areas, we know them to be the authoritative source of risk assessment techniques and risk mitigation measures. For example, insurance actuaries know that anti-lock brakes deserve a $14 discount on monthly premiums, and that 15 minutes of daily exercise can reduce the chance of heart attack by 22%.[9] But from my research investigating cyber insurance policies[10], it appears that these insurance carriers do not have the sophistication and granular information when it comes to assessing cyber risk. For example, some insurers provide firms with a questionnaire that is ostensibly used to assess cyber risk, but the actual rate schedules (the formulas used to determine the premiums) use a set of variables multiplied together that may or may not include information about a firm's security posture. In fact, many of the factors driving cyber insurance premiums relate to the size of the company (as measured by total assets or revenues), industry, requested limits and retention, and other variables that are unrelated to adopting security precautions.

All this suggests that at least in the area of cyber risk, the insurance industry is doing no better than the security professionals at answering basic questions. But hope is not lost. Cyber insurance is a new area, and it takes time to understand how to assess and price cyber risk. Carriers and reinsurers may eventually discover which security controls work best. They don't currently, but they are the entity that has the best opportunity to make significant innovations. They will be able to perform statistical analyses of their data that takes advantage of variations in the security controls. If there are differences between the precautions taken by firms that suffered a loss and those that did not, insurers will suss out those differences and promote the security controls that are best able to prevent losses.

There will be many entities that benefit from better knowledge and more precise risk assessment: carriers will enjoy increased profits, firms will suffer fewer breaches, and consumers will bear fewer losses from identity theft and other harms.

VI. Valuing Consumer Data and Consumer Harm

Over 2017 and 2018, the FTC hosted a number of workshops related to consumer data protection and privacy.[11] Part of these discussions are meant to inform an agenda related to taking a harm-based approach to public enforcement. If we can properly identify and quantify the harms borne by consumers, this would help justify bringing sanctions against the firms that handled (or mishandled) their data.

---

[9] These figures are entirely fictional.

[10] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk? (forthcoming in the Journal of Cybersecurity).

[11] See https://www.ftc.gov/policy/hearings-competition-consumer-protection.

If there is one consistent theme that has run across the FTC workshops, it is that experts in multiple disciplines continue to struggle with defining privacy and security harms. At best, we have realized that informed consent (notice and choice) do not work well,[12] and that alternatives to informed consent are scarce and poorly defined. Perhaps the fact that we spend so much time hunting for an answer should tell us something about the nature of the problem.

Data security harms, which should have less complexity than privacy harms since there are no countervailing benefits to the consumer when a breach occurs, can nevertheless be elusive. To be clear, this isn't to suggest that identity theft isn't real. Some people do suffer tremendously from it, and every step should be taken to make these victims whole again. But it appears that most people do not suffer any concrete, articulable harms from data breaches. [13] And until we can identify and quantify data breach harms to boardroom executives, policy makers, and judges, firms will continue to invest in security and privacy controls that minimize their own costs. Policy interventions will remain only weakly targeted, enforceable and effective until lawmakers understand whether an externality does indeed exist, and how to induce firms to internalize those costs.

Returning for a moment to the discussion of enterprise risk and the role of the FTC, there exists an important tension. On one hand, we want firms to address cyber like any other enterprise risk, which, as we discussed, could mean that cyber will be deprioritized if it is reasonably determined to pose a lesser concern relative to other enterprise risks faced by the company. On the other hand, the FTC may bring an enforcement action against a company if it suffers a breach even if it has taken the efficient level of precaution.[14]

And so what is the firm to do? Invest in a heightened level of security so as to not draw the attention of the FTC, or invest in a level of security commensurate with a well-reasoned enterprise risk management assessment, even though that level may be lower?

---

[12] Ben-Shahar, O., & Schneider, Carl E. (2014) More Than You Wanted to Know The Failure of Mandated Disclosure. Princeton Press.

[13] See Ponemon (2014) showing that only 13% of data breach victims suffered financial loss (available at https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf) and the Bureau of Justice Statistics showing that in 2016, only 12% of identity theft victims suffered any kind of out of pocket expense (available at https://www.bjs.gov/content/pub/pdf/vit16_sum.pdf). Further, the Identity Theft Resource Center estimates that 179 million records were compromised in 2017 (https://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReport2017c.pdf), while Javelin Research estimates that 16.7 million people suffered some form of identity fraud (https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin). Together, these two data points suggest that only 9.3% (16.7m / 179m) of breach victims suffered identity fraud. Note that both figures are estimates, and that the reported total number of victims may be both under-estimated (given that not all reported breaches recorded the number of lost records), and over-estimated (given that one person's information may have been compromised multiple times). Further, the reported number of fraud victims (16.7m) may be overestimated given that not all victims suffered actual financial loss. All documents last accessed January 7, 2019.

[14] See LabMD, Inc. v. FTC, No. 16-16270 (11th Cir. June 6, 2018), http://media.ca11.uscourts.gov/opinions/pub/files/201616270.pdf.

Now, perhaps the answer is clear: the firm should take the enterprise risk management approach, and be sure to incorporate not only its existing security controls and threat landscape into the decision, but also the expected losses from any private or public enforcement action that it might endure in the event of a breach as a result of its actions. This appears straightforward in theory, but it is entirely unclear whether firms are indeed so thoughtful and calculating when addressing these issues. To make matters worse, this becomes even more complicated with regulators like the FTC whose enforcement actions do not simply require the firms to pay back the consumers the market value of the breach (which is not much), but usually also push the firm into an intensive settlement contract and/or threaten fines that may exceed the market value of the harm.

Conclusion

This white paper has surveyed the terrain to show the gaps in the tool set used to assess cyber risks and resulting harms. It has challenged the conventional wisdom that firms are not investing enough in cybersecurity, and proposed that to the extent there is waste, consumers should also bear some responsibility (to the extent they can) to protect their own information using efficient precautions. While it seems appropriate that cyber threats should be managed similarly to other forms of enterprise risk, this could lead to a rational decision to reduce investment in cybersecurity, even if it may lead to FTC or other regulatory enforcement actions. Finally, I discussed the current state of cyber insurance, which offers few insights today but holds great promise for being able to solve some of the most pressing issues in cybersecurity in the future.

While the FTC has invested a great deal of time in bringing experts together to testify in their 2017 and 2018 hearings in an effort to inform regulators and the public, a number of questions still remain. In order to make evidence-based policies, emphasis should be placed on finding answers to the following questions that have plagued the information security industry for decades:

- How do we measure cyber risk? How will I know whether I am more secure today vs a year from now?
- Given a certain budget, which security controls will provide the greatest marginal improvements at reducing risk, and by how much?
- How can we most effectively understand and, ideally, quantify consumer harms?

Any efforts to obtain better answers to these questions will materially advance our understanding of how to best invest in data security efforts, and how to best design and apply corporate and public policies.